IF3



PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# TRANSMITTAL FORM

*(to be used for all correspondence after initial filing)*

| | | | |
|---|---|---|---|
| | | Application Number | 10/708,949 |
| | | Filing Date | 04/02/2004 |
| | | First Named Inventor | Chen-Huang FAN |
| | | Art Unit | |
| | | Examiner Name | |
| Total Number of Pages in This Submission | 3 | Attorney Docket Number | ACMP0048USA |

## ENCLOSURES *(Check all that apply)*

- ☑ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

| | |
|---|---|
| Firm or Individual name | Winston Hsu, Reg. No.: 41,526 |
| Signature | Winston Hsu |
| Date | 6/28/2004 |

## CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

| | | | |
|---|---|---|---|
| Typed or printed name | | | |
| Signature | | Date | |

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# FEE TRANSMITTAL for FY 2004

*Effective 10/01/2003. Patent fees are subject to annual revision.*

☐ Applicant claims small entity status. See 37 CFR 1.27

| TOTAL AMOUNT OF PAYMENT | ($) 0.00 |
|---|---|

| Complete if Known | |
|---|---|
| Application Number | 10/708,949 |
| Filing Date | 04/02/2004 |
| First Named Inventor | Chen-Huang FAN |
| Examiner Name | |
| Art Unit | |
| Attorney Docket No. | ACMP0048USA |

## METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-3105

Deposit Account Name: North America Intellectual Property Corp.

**The Director is authorized to:** *(check all that apply)*

☑ Charge fee(s) indicated below ☐ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

## FEE CALCULATION

### 1. BASIC FILING FEE

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 1001 | 770 | 2001 | 385 | Utility filing fee | |
| 1002 | 340 | 2002 | 170 | Design filing fee | |
| 1003 | 530 | 2003 | 265 | Plant filing fee | |
| 1004 | 770 | 2004 | 385 | Reissue filing fee | |
| 1005 | 160 | 2005 | 80 | Provisional filing fee | |

SUBTOTAL (1) ($) 0.00

### 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

| | Extra Claims | | Fee from below | | Fee Paid |
|---|---|---|---|---|---|
| Total Claims | | -20** = | | X | = |
| Independent Claims | | - 3** = | | X | = |
| Multiple Dependent | | | | | = |

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description |
|---|---|---|---|---|
| 1202 | 18 | 2202 | 9 | Claims in excess of 20 |
| 1201 | 86 | 2201 | 43 | Independent claims in excess of 3 |
| 1203 | 290 | 2203 | 145 | Multiple dependent claim, if not paid |
| 1204 | 86 | 2204 | 43 | ** Reissue independent claims over original patent |
| 1205 | 18 | 2205 | 9 | ** Reissue claims in excess of 20 and over original patent |

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 1051 | 130 | 2051 | 65 | Surcharge - late filing fee or oath | |
| 1052 | 50 | 2052 | 25 | Surcharge - late provisional filing fee or cover sheet | |
| 1053 | 130 | 1053 | 130 | Non-English specification | |
| 1812 | 2,520 | 1812 | 2,520 | For filing a request for *ex parte* reexamination | |
| 1804 | 920* | 1804 | 920* | Requesting publication of SIR prior to Examiner action | |
| 1805 | 1,840* | 1805 | 1,840* | Requesting publication of SIR after Examiner action | |
| 1251 | 110 | 2251 | 55 | Extension for reply within first month | |
| 1252 | 420 | 2252 | 210 | Extension for reply within second month | |
| 1253 | 950 | 2253 | 475 | Extension for reply within third month | |
| 1254 | 1,480 | 2254 | 740 | Extension for reply within fourth month | |
| 1255 | 2,010 | 2255 | 1,005 | Extension for reply within fifth month | |
| 1401 | 330 | 2401 | 165 | Notice of Appeal | |
| 1402 | 330 | 2402 | 165 | Filing a brief in support of an appeal | |
| 1403 | 290 | 2403 | 145 | Request for oral hearing | |
| 1451 | 1,510 | 1451 | 1,510 | Petition to institute a public use proceeding | |
| 1452 | 110 | 2452 | 55 | Petition to revive - unavoidable | |
| 1453 | 1,330 | 2453 | 665 | Petition to revive - unintentional | |
| 1501 | 1,330 | 2501 | 665 | Utility issue fee (or reissue) | |
| 1502 | 480 | 2502 | 240 | Design issue fee | |
| 1503 | 640 | 2503 | 320 | Plant issue fee | |
| 1460 | 130 | 1460 | 130 | Petitions to the Commissioner | |
| 1807 | 50 | 1807 | 50 | Processing fee under 37 CFR 1.17(q) | |
| 1806 | 180 | 1806 | 180 | Submission of Information Disclosure Stmt | |
| 8021 | 40 | 8021 | 40 | Recording each patent assignment per property (times number of properties) | |
| 1809 | 770 | 2809 | 385 | Filing a submission after final rejection (37 CFR 1.129(a)) | |
| 1810 | 770 | 2810 | 385 | For each additional invention to be examined (37 CFR 1.129(b)) | |
| 1801 | 770 | 2801 | 385 | Request for Continued Examination (RCE) | |
| 1802 | 900 | 1802 | 900 | Request for expedited examination of a design application | |

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

## SUBMITTED BY

(Complete *(if applicable)*)

| Name (Print/Type) | Winston Hsu | Registration No. (Attorney/Agent) | 41,526 | Telephone | 886289237350 |
|---|---|---|---|---|---|
| Signature | Winston Hsu | | | Date | 6/24/2004 |

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*

PTO/SB/02B (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

# DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

| Prior Foreign Application Number(s) | Country | Foreign Filing Date (MM/DD/YYYY) | Priority Not Claimed | Certified Copy Attached? | |
|---|---|---|---|---|---|
| | | | | YES | NO |
| 092107825 | Taiwan R.O.C | 04/04/2003 | ☐ | ☑ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |
| | | | ☐ | ☐ | ☐ |

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

ACM-98

# 中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder :

申　　請　　日 ： 西元 2003 年 04 月 04 日
Application Date

申　請　案　號 ： 092107825
Application No.

申　　請　　人 ： 明基電通股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2003 年 5 月 14 日
Issue Date

發文字號： 09220483040
Serial No.

| 申請日期： | IPC分類 |
| --- | --- |
| 申請案號： | |

（以上各欄由本局填註）

# 發明專利說明書

| | | |
| --- | --- | --- |
| 一、發明名稱 | 中 文 | 以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置 |
| | 英 文 | Network Lock Method And Related Apparatus By Ciphered Network Lock And Inerasable Deciphering Key |
| 二、發明人（共3人） | 姓 名（中文） | 1. 范振煌<br>2. 杜本權 |
| | 姓 名（英文） | 1. Fan, Chen-Huang<br>2. Du, Ben-Chuan |
| | 國 籍（中英文） | 1. 中華民國 TW 2. 中華民國 TW |
| | 住居所（中 文） | 1. 苗栗縣頭份鎮尖豐路五十二號<br>2. 台北縣新店市三民路七十五巷九弄十二號二樓 |
| | 住居所（英 文） | 1. No. 52, Jian-Feng Rd., Tou-Fen Town, Miao-Li Hsien, Taiwan, R.O.C.<br>2. 2F, No.12, Alley 9, Lane 75, San-Min Rd., Hsin-Tien City, Taipei Hsien, Taiwan, R. |
| 三、申請人（共1人） | 名稱或姓 名（中文） | 1. 明基電通股份有限公司 |
| | 名稱或姓 名（英文） | 1. BenQ Corporation |
| | 國 籍（中英文） | 1. 中華民國 TW |
| | 住居所（營業所）（中 文） | 1. 桃園縣龜山鄉山鶯路157號 （本地址與前向貴局申請者相同） |
| | 住居所（營業所）（英 文） | 1. No. 157, Shan-Ying Road, Kweishan, Tao-Yuan Hsien, Taiwan, R.O.C. |
| | 代表人（中文） | 1. 李焜耀 |
| | 代表人（英文） | 1. Lee, Kuen-Yao |

| | |
|---|---|
| 申請日期： | IPC分類 |
| 申請案號： | |

（以上各欄由本局填註）

# 發明專利說明書

| | | |
|---|---|---|
| 一、發明名稱 | 中 文 | |
| | 英 文 | |
| 二、發明人（共3人） | 姓 名（中文） | 3. 程意雯 |
| | 姓 名（英文） | 3. Cheng, Yi-Wen |
| | 國 籍（中英文） | 3. 中華民國 TW |
| | 住居所（中 文） | 3. 台北市光復南路十三巷四十三號二樓 |
| | 住居所（英 文） | 3. 2F, No. 43, Lane 13, Kuang-Fu S. Rd., Taipei City, Taiwan, R.O.C. |
| 三、申請人（共1人） | 名稱或姓 名（中文） | |
| | 名稱或姓 名（英文） | |
| | 國 籍（中英文） | |
| | 住居所（營業所）（中 文） | |
| | 住居所（營業所）（英 文） | |
| | 代表人（中文） | |
| | 代表人（英文） | |

四、中文發明摘要　（發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置）

本發明提供一種無線通信網路之網路鎖保護方法及相關裝置。該方法係將不同的手機對應於一非對稱密碼演算法之相異加密金鑰及解密金鑰；對應一手機網路鎖之存取資料內容會根據對應之加密金鑰以一非對稱密碼演算法加密後儲存於該手機中，而解密所用之解密金鑰則儲存於該手機的防寫記憶體中，使該解密金鑰不會被覆寫；而該明文存取資料及該加密金鑰則僅記錄於該無線通信網路之服務提供端中。要實施網路鎖時，該手機會以防寫記憶體中之解密金鑰將加密之存取資料內容解密以驗證該手機是否能存取該無線通信網路之通信服務。

伍、（一）、本案代表圖為：第 3圖

（二）、本案代表圖之元件代表符號簡單說明：

30　通信網路　32A-32B 手機

六、英文發明摘要　（發明名稱：Network Lock Method And Related Apparatus By Ciphered Network Lock And Inerasable Deciphering Key）

A protection method and related apparatus for network lock of a communication network. The method includes: associating different cell phones to different enciphering and deciphering keys of an asymmetric encryption algorithm. An access information of a network lock corresponding to a cell phone is enciphered by the corresponding enciphering key. Then the

四、中文發明摘要　（發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置）

| | | | |
|---|---|---|---|
| 36 | 處理器 | 50A-50B | 防寫記憶體 |
| 40A-40B | 資料記憶體 | 52 | 資料庫 |
| 54 | 密碼演算法 | IDA-IDB | 裝置識別碼 |
| EKA-EKB | 加密金鑰 | DKA-DKB | 解密金鑰 |
| PTA-PTB、PTA2 | | | 明文存取資料 |
| CTA-CTB | 密文存取資料 | | |

六、英文發明摘要　（發明名稱：Network Lock Method And Related Apparatus By Ciphered Network Lock And Inerasable Deciphering Key ）

enciphered network lock is stored in the cell phone, and the corresponding deciphering key is recorded in an inerasable memory of the cell phone. The original plaintext access information of the network lock and the enciphering key is stored only in a service provider of the communication network. When the cell phone tries to access the communication network, it

四、中文發明摘要　（發明名稱：以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置）

六、英文發明摘要　（發明名稱：Network Lock Method And Related Apparatus By Ciphered Network Lock And Inerasable Deciphering Key ）

deciphered the enciphered network lock using the deciphering key stored in the inerasable memory to verify the network lock of the cell phone.

一、本案已向

國家(地區)申請專利　　申請日期　　案號　　主張專利法第二十四條第一項優先權

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構:　　無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期:　　無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明（1）

發明所屬之技術領域

本發明係提供一種網路鎖保護方法及相關裝置，尤指一種將解密金鑰儲存於手機中之防寫記憶體、並以該解密金鑰將加密後之網路鎖資料內容解密以驗證網路鎖機制之網路鎖保護方法及相關裝置。

先前技術

在資訊發達的現代社會中，便利的無線通信網路已為人際交流、資訊交換最重要的途徑之一。只要以方便輕巧、操作簡便的手機，人人都能輕易地利用無線通信網路中的通信服務，隨時隨地享受無遠弗屆的資訊存取能力。為了使通信網路能永續經營，提高通信服務之品質，如何維持通信網路中的通信秩序，並確保通信網路中用戶的權益，也就成了現代資訊業界研發的重點之一。

一般來說，無線通信網路中的通信服務是由網路服務端提供的，手機的使用者則付費成為網路服務端的合用戶，並得以使用網路服務端提供的通信服務。為了要確保合法用戶的權益，當手機的使用者要以手機來存取通信服務時，手機會透過一網路鎖機制驗證使用者是否為合法之用戶；若使用者並非合法用戶，手機本身就

會限制使用者對通信網路的存取。關於此情形，請參考圖一。圖一為一習知通信系統10中，各通信裝置（如手機12、13）與一服務提供端28配置的示意圖。以手機12做為代表來說明習知通信系統10之通信裝置，手機12中設有一無線電訊號之收發模組14、一主控手機運作的處理器16、一用來記錄資料的資料記憶體20（譬如說是快閃記憶體等非揮發性記憶體）、一用來識別用戶身份的用戶識別卡24、一用來將聲波轉換為電子訊號的麥克風18A、一揚聲器18B以及人機介面21。人機介面21可包含鍵盤、顯示器、振動器等等，讓手機12的使用者得以透過人機介面21操控手機12，並由人機介面21得知手機12運作的情形。服務提供端28則設有收發傳輸無線電訊號的基地台29，以在各手機間傳輸無線電訊號，提供通信服務。舉例來說，手機12使用者的語音聲波可由麥克風18A接收並轉為電子訊號，由處理器16將其適當地編碼（encoding），再傳輸到收發模組14中進一步調變為射頻訊號，由收發模組14以無線電形式發射至基地台29。基地台29接收手機12發出之無線電訊號後，就可將此訊號再透過基地台29以無線電的方式傳輸至手機13，讓手機13的使用者可接收到手機12使用者傳來的訊息。同理，手機13要傳輸至手機12的語音訊息，也會以無線電方式透過基地台29的轉接傳輸至手機12，由手機12的收發模組14接收並解調為基頻訊號，再由處理器16適當地解碼（decoding），傳輸至揚聲器18B，轉換成聲波語音播放出

來，讓手機12的使用者能夠聽到。如此一來，手機12、13之使用者就能透過服務提供端28提供的通信服務相互溝通。

然而，正如前述，為了維護通信網路10合法用戶的正當權利，在手機12要存取通信網路10的通信服務前，手機12還會自動進行一驗證步驟，以驗證手機12的使用者是否能合法存取通信網路10的通信服務。為了配合此一驗證步驟的進行，手機12中的用戶識別卡（即所謂的SIM卡）24記錄有一用戶識別碼26，用來代表手機12使用者的身份。一般來說，用戶識別卡24是以可插拔的方式安裝於手機12中；當一使用者要使用手機12來存取通信網路10時，就要將其持有的用戶識別卡24插入安裝於手機12中，讓手機12可辨識使用者的身份。對應於用戶識別卡24中的用戶識別碼26，資料記憶體20中除了記錄手機12運作所必需的資料外（像是手機12的韌體），也記錄有一裝置識別碼23，及用來進行驗證步驟的存取資料22。其中裝置識別碼23為各手機獨有的專屬識別碼（像是IMEI識別碼，International Mobile Equipment Identity）；換句話說，不同的手機，其所具有的裝置識別碼也不同。而存取資料22即用來記錄手機12網路鎖的狀態。所謂的網路鎖，就是用來定義手機12是否僅能接受某些用戶識別碼來存取通信網路10的通信服務。而存取資料22中，即記錄了網路鎖是否啟動，以及手機12

五、發明說明 (4)

可接受之合法用戶識別碼。舉例來說，當用戶識別碼 26中某些欄位之值在某一預設範圍中時，手機 12可接受其為合法之用戶識別碼；而該預設範圍即記錄於存取資料 22中。在習知技術中，當手機 12要進行驗證步驟時，處理器 16會由資料記憶體 20中讀取存取資料 22，根據存取資料 22來判斷手機 12的網路鎖是否啟動。若存取資料 22中記錄網路鎖是啟動的，處理器 16會進一步檢查用戶識別卡 24中的用戶識別碼 26是否在存取資料 22記錄之合法用戶識別碼中。若用戶識別碼 26符合合法用戶識別碼（舉例來說，承前所述，用戶識別碼 26中某些欄位之值在存取資料 22記錄之預設範圍中），處理器 16就會判斷用戶識別卡 24的持有者為通信網路 10的合法使用者，並使手機 12能繼續進行後續的步驟，讓手機 12的使用者（也就是用戶識別碼 24的持有者）能透過手機 12存取通信網路 10的通信服務。反之，若處理器 16比對發現用戶識別卡 24中的用戶識別碼 26並不在存取資料 22記錄之合法用戶識別碼範圍之內，處理器 16就會判斷用戶識別卡 24之持有者並非通信網路 10的合法使用者，並使手機 12停止對通信網路 10的存取。另一方面，若進行驗證步驟時處理器 16發現存取資料 22中記錄網路鎖並沒有啟動，理器 16就不會檢查用戶識別碼 26，而直接允許用戶識別卡 24之持有者透過手機 12存取通信網路 10之通信服務。

簡而言之，上述之習知網路鎖的實現方式，即是依靠資料記憶體20中儲存的存取資料22來判斷用戶識別卡24的持有者是否能透過手機12存取通信網路10的通信服務。然而，此種習知的方法也隱含了網路鎖被非法使用者破解的危機。舉例來說，當一非法使用者要破解手機12的網路鎖時，非法使用者可以由網路鎖沒有被啟動的其他手機中取得其存取資料；由於此類手機中的網路鎖沒有啟動，此存取資料中會記錄網路鎖為不啟動，而此存取資料即可做為一破解存取資料。即使手機12的存取資料22中記錄手機12的網路鎖為啟動，但非法使用者可破解存取資料覆寫至資料記憶體20中，將原來的存取資料22覆蓋(overwrite)，以此破解存取資料來取代原來的存取資料22。等到手機12要進行驗證步驟時，就會錯誤地根據破解存取資料而不啟動網路鎖，而手機12的網路鎖也就被破解了。此時即使用戶識別卡24上的用戶識別碼26並非合法用戶識別碼，用戶識別碼24的持有者也可非法地以手機12來存取通信網路10的通信服務。在技術層面上，為了方便對手機12的維修、測試，手機12中的資料記憶體20會設有維修用的預設接點，而非法使用者就可利用這些預設接點以特殊的資料燒錄工具（像是TAG tool）將破解存取資料寫入至資料記憶體20並覆蓋原來的存取資料22，以破解手機12的網路鎖。尤有甚者，非法使用者還能直接改寫存取資料22中的記錄，譬如說將存取資料22中原本記錄為啟動的網路鎖改為不啟

動，也能破解手機12的網路鎖。另外，非法使用者還能刪除存取資料22。一般來說，在習知之手機12中，當處理器16發現資料記憶體20中沒有存取資料22時，會根據一預設的存取資料來進行網路鎖之驗證步驟，而此預設存取資料多半不會啟動網路鎖之功能。這樣一來，非法使用者也能破解手機12的網路鎖。一旦網路鎖被非法破解，就會影響通信網路10的通信秩序，損及服務提供端及各合法用戶（合法用戶識別卡之持有者）的權益。

## 發明內容

因此，本發明之主要目的，即在於提供一種安全性較高的網路鎖保護機制及相關系統、裝置，以克服習知網路鎖機制易遭破解的缺點。

在習知的網路鎖機制中，手機中的處理器是依據資料記憶體中存取資料所記錄之網路鎖狀態來進行網路鎖的驗證步驟；一旦存取資料被覆寫、竄改，網路鎖就會被破解，影響通信網路中的正常秩序及各方的合法權益。

在本發明中，係以一非對稱性的密碼演算法，針對不同的手機以不同的加密金鑰將各手機網路鎖之存取資料加密為密文存取資料，各手機中僅儲存密文存取資

料，並以一防寫記憶體記錄解密之對應解密金鑰；而各手機對應的加密金鑰則僅保留於服務提供端之資料庫中。其中該防寫記憶體為一單次寫入(OTP，One-Time Programmable)記憶體或為一快閃記憶體之可鎖定(lockable)記憶區，以使記錄於其中的解密金鑰不會被覆寫。當一手機要進行驗證步驟時，該手機會根據該防寫記憶體中的解密金鑰將資料記憶體中的密文存取資料解密為明文存取資料，並根據明文存取資料中記錄的網路鎖狀態來進行相關之網路鎖驗證。由於各手機對應的加解密金鑰皆互不相同，且各手機中的解密金鑰無法被改寫，即使非法使用者意圖破解某一手機A之網路鎖而將另一手機B中記錄的密文存取資料覆寫至手機A中，但當手機A進行驗證步驟而將該密文存取資料解密時，會因為手機A、B之解密金鑰不同而使手機A無法解出正確格式的明文存取資料，此時手機A即可判斷網路鎖已遭破壞，可以停止對通信網路的存取，以防止通信網路之正常秩序受不法侵害。由於各手機中儲存的存取資料為密文之存取資料，也可防止非法使用者以直接修改存取資料的方式來破解網路鎖。由於加密金鑰並不會暴露於各手機或通信網路中，即使非法使用者能竄改明文存取資料，也無法以正確的加密金鑰將竄改後之明文存取資料加密為對應解密金鑰的正確密文存取資料。另外，當服務提供端要更新一手機中的網路鎖存取資料時，可由資料庫中找出該手機對應的加密金鑰，將更新的明文存取資料加

密為新的密文存取資料，再將此一更新後之密文存取資料存入該手機的資料記憶體中。經由上述機制，本發明將可確保各手機中網路鎖的安全，進一步維護通信網路中的正常秩序及各方的合法權益。

實施方式

請參考圖二。圖二為本發明通信網路30配置的示意圖。通信網路30可以是一無線通信網路，以服務提供端48提供通信服務，而各使用者則透過各手機（圖二中繪兩手機32A、32B做為代表）來存取通信網路30的通信服務。以手機32A做為代表來說明通信網路30中各手機的構造；手機32A做為一通信裝置，其包括有一用來收發無線電訊號的收發模組34、一用來控制手機12運作之處理器36、一用來將聲波轉換為電子訊號的麥克風38A、一用來將電子訊號轉換為聲波的揚聲器38B、一用來以非揮發性方式儲存資料的資料記憶體40A、一非揮發性的防寫記憶體50A、一以可插拔方式安裝於手機32A中的客戶識別卡45，以及一人機介面（MMI，Man-Machine Interface)41。人機介面41可以包括有鍵盤、顯示器、一來提示來電的振動器及另一揚聲器等等，讓手機32A的使用者可透過此人機介面41操控手機32A，並由顯示器等介面得知手機32A的運作狀態。服務提供端48則設有多個基地台49，用來向各手機收發無線電訊號，以向各手機

提供通信服務。舉例來說，手機32A使用者的語音聲波可經由麥可風38A接收轉為電子訊號，經由處理器36的編碼、訊號處理後傳輸至收發模組34，由收發模組34將其調變為射頻訊號後，以無線電的方式發射至服務提供端48的基地台49。服務提供端48在接收手機32A傳來的無線電訊號後，可透過另一基地台49將手機32A的訊號再以無線電方式傳輸至手機32B，讓手機32B的使用者能經由服務提供端48的通信服務而接收到手機32A使用者傳來的訊息。同理，手機32B的訊息也能經由服務提供端48訊號轉接之通信服務而傳至手機32A的收發模組34，由收發模組34將其解調為基頻訊號，再由處理器36進一步解碼、訊號處理，並由揚聲器38B將其以聲波的方式播放出來（或經由人機介面41顯示出來）。

不過，如前所述，為了維持通信網路30正常的通信秩序及各使用者的合法權益，在手機32A的使用者在透過手機32A存取通信網路30的通信服務前，要先在手機32A中插入其所持有的用戶識別卡45，而手機32A就會依據用戶識別卡45上記錄的用戶識別碼46自動地進行一驗證步驟，以透過網路鎖的機制驗證手機32A的使用者（亦即用識別卡45的持有者）是否為通信網路30的合法用戶，並決定是否要繼續存取通信服務。為了配合本發明驗證機制的實施，在本發明通信網路30中，各手機的資料記憶體除了儲存代表各手機的裝置識別碼（及各手機的韌

體）外，還儲存有一密文存取資料；而各手機也另設有一防寫記憶體，用來儲存一對應的解密金鑰。如圖二所示，手機32A的資料記憶體40A中即儲存有手機32A的裝置識別碼IDA及一密文存取資料CTA；而其防寫記憶體50A中則儲存有一解密金鑰DKA。基於相同的配置原理，手機32B中的資料記憶體40B則儲存有對應手機32B的裝置識別碼IDB、密文資料CTB，並於其防寫記憶體50B中儲存有一解密金鑰DKB（手機32A的基本構造與手機32A相似，在不妨礙本發明技術揭露的情形下，手機32B的部分構造，如收發模組、處理器等等已於圖二中省略未示）。如前所述，各手機對應的裝置識別碼（像是IMEI識別碼）係用來獨一無二地識別出該手機，故不同的手機也具有不同的裝置識別碼，如手機32A的裝置識別碼IDA就和手機32B的裝置識別碼IDB不同。另外，在通信網路30中，不同手機中記錄的解密金鑰、密文存取資料也互不相同。以圖二為例，各手機32A、32B對應的解密金鑰DKA、DKB以及密文存取資料CTA、CTB即互不相同。其中，各手機的解密金鑰是儲存於防寫記憶體中的。此防寫記憶體的特性即是其內記錄的資料具有唯讀的特性；一旦資料被燒錄記錄於防寫記憶體後，該資料即無法再被覆寫。在實際施時，此防寫記憶體可以是單次可程化（OTP，One-Time Programmable)記憶體；一旦資料被寫入防寫記憶體後，該資料就不能被覆寫而具有唯讀（read-only）的特性。另外，在現代的某些快閃記憶體中，已經可劃

分出部分的記憶區為可鎖定（lockable)的記憶區；同樣地，資料被燒錄、寫入至此可鎖定之記憶區後，就不能再被覆寫而具有唯讀的特性。相對地，在同一快閃記憶體不具有可鎖定特性之記憶區中，資料還是可被重複寫入、抹除。利用這樣的快閃記憶體，本發明中的資料記憶體、防寫記憶體就能實施於同一快閃記憶體上，其中可鎖定之記憶區做為防寫記憶體，用來記錄各手機對應的解密金鑰；不具有可鎖定特性而可重複覆寫的記憶區，即可當作資料記憶體，以記錄手機的韌體及裝置識別碼、密文存取資料等等。

配合本發明的實施，本發明於服務提供端48也設有一資料庫52，用來記錄各手機對應之裝置識別碼、一對應之加密金鑰及一明文存取資料，也可選擇性地記錄各手機對應的解密金鑰。舉例來說，針對圖二中的兩手機32A、32B，資料庫52即記錄了手機32A的裝置識別碼IDA，並以裝置識別碼IDA為記錄的索引標的，記錄了手機32A對應之加密金鑰EKA、解密金鑰DKA及明文存取資料PTA。同理，針對手機32B，資料庫48中也以手機32B之裝置識別碼IDB做為記錄索引之標的，記錄了手機32B對應加密金鑰EKB、解密金鑰DKB以及明文存取資料PTB。其中，對應各手機的明文存取資料，就是用來記錄該手機網路鎖之存取資料內容，像是網路鎖是否啟動，網路鎖所能接受之合法用戶識別碼等等。

本發明網路鎖機制實施的原理可先描述如下。本發明是將各手機網路鎖的存取資料根據該手機對應之加密金鑰以一非對稱之密碼演算法加密，成為該手機資料記憶體中之密文存取資料。等到該手機在存取通信服務前而要進行驗證步驟時，該手機之處理器即以防寫記憶體中的解密金鑰將密文存取資料解密為明文存取資料，再依據明文存取資料中記錄的事項（如網路鎖是否啟動，合法用戶識別碼之範圍）來比對該手機之用戶識別卡持有者是否為合法用戶，實現網路鎖機制。至於本發明進步的實施細節，請繼續參考圖三（並一併參考圖二）。圖三為本發明於通信網路30中進行網路鎖驗證機制的示意圖。為了方便後續說明，簡化圖式，在不妨礙本發明技術揭露的情形下，圖三中手機32A、32B的部分裝置（如收發模組等等）已經省略未繪出。

承前所述，本發明在實施時會以一預設之非對稱密碼演算法將明文存取資料、密文存取資料加解密。在非對稱之密碼演算法中，將一明文加密為一密文的加密金鑰，與將該密文解密為原來明文所需的對應解密金鑰，者並不相同。換句話說，當明文以加密金鑰加密為對應的密文後，該密文無法以同一個加密金鑰解密為原來的明文，必需要經由對應的特定解密金鑰才能解密為原來的明文。同理，以該解密金鑰對該明文加密所得出的

結果，和以該加密金鑰對該明文加密所得出的密文，兩者也不會相同。根據此密碼演算法，本發明可預先算出複數組不同的加密金鑰及對應之解密金鑰，各組的加密金鑰均不相同。配合各手機的出廠，各手機會被賦予專屬的對應裝置識別碼，而本發明即可利用各手機的裝置識別碼做為記錄索引標的，將一組加密金鑰及對應之解密金鑰指定予一手機，並連同該手機對應的明文存取資料，一同記錄於服務提供端48的資料庫52中。如圖三中的示意例，本發明可於服務提供端48預先根據非對稱的密碼演算法54計算出加密金鑰EKA及其對應之解密金鑰DKA、加密金鑰EKB及對應之解密金鑰DKB等等。其中加密金鑰EKA、EKB相異；再加上密碼演算法54的非對稱特性，事實上加解密金鑰EKA、EKB、DKA、DKB皆不相同。當手機32A出廠時，手機32A會被賦予其專屬之裝置識別碼IDA；而服務提供端48也就可以將加密金鑰EKA、解密金鑰DKA分配予手機32A，並以手機32A之裝置識別碼IDA為記錄索引標的，將加解密金鑰EKA、DKA連同手機32A網路鎖對應之明文存取資料PTA一同記錄於資料庫52中。同理，對應於裝置識別碼為IDB的手機32B，服務提供端48可將加解密金鑰EKB、DKB分配予手機32B；並在資料庫52，將加解密金鑰EKB、DKB連同手機32B網路鎖對應之明文存取資料PTB，一同記錄於裝置識別碼IDB對應之項目下。

五、發明說明 (14)

在服務提供端48中，除了在各手機出廠時將不同組的加解密金鑰分配給各手機，也會將各手機對應之解密金鑰寫入至該手機的防寫記憶體中。等手機出廠後而為各使用者使用時，各手機中記錄的解密金鑰也就不能被覆寫了。如圖三所示，手機32A的對應解密金鑰DKA會被記錄於防寫記憶體50A中，並具有不可覆寫的唯讀特性。同樣地，手機32B中的防寫記憶體50B中也以唯讀特性記錄了手機32B對應的解密金鑰DKB。另外，在資料庫52的各筆明文存取資料，就以明文記錄了各對應手機的網路鎖狀態。然而，在本發明中，各手機網路鎖之明文存取資料並不會直接儲存於各手機中，而是會由服務提供端48根據各手機對應之加密金鑰以密碼演算法54加密為密文存取資料，再將此密文存取資料寫入至對應手機的資料記憶體32A中。　　如圖三中，各手機32A、32B對應之明文存取資料PTA、PTB，即分別用來以明文記錄對應手機網路鎖之狀態。舉例來說，明文存取資料PTA記錄了手機32A的網路鎖功能是否啟動等等相關訊息。不過，如前所述，服務提供端48會先根據手機32A之加密金鑰EKA，以密碼演算法54將手機32A之明文存取資料PTA加密為密文存取資料CTA，再將密文存取資料CTA記錄於手機32A的資料記憶體40A中。同理，服務提供端48也會根據手機32B對應之加密金鑰EKB，以密碼演算法54將手機32B對應之明文存取資料PTB加密為對應的密文存取資料CTB，再將密文存取資料CTB寫入至手機32B的資料記憶體40B中。

總結以上描述，在手機32A出廠時，資料庫52中已經記錄有手機32A對應的加解密金鑰EKA、DKA及網路鎖的明文存取資料PTA；手機32A中也已經於防寫記憶體50A中以唯讀、不可覆寫之特性記錄有手機32A的解密金鑰DKA，並於資料記憶體40A中記錄有密文存取資料CTA。同理，在手機32B出廠而能為使用者使用時，手機32B中的防寫記憶體50B也以唯讀特性記錄了手機32B的解密金鑰DKB，手機32B的資料記憶體40B中也記錄有手機32B的密文存取資料CTB。請注意，在本發明的架構下，各手機雖有各自對應的加密金鑰及網路鎖明文存取資料，但這些資料均僅記錄於服務提供端48的資料庫52中，不會暴露於各手機中；而各手機中僅保存有對應的密文存取資料及解密金鑰。

簡而言之，在本發明架構下，當各手機出廠而能為各使用者使用時，各手機中已經儲存有該手機對應的解密金鑰及密文存取資料。如前所述，當使用者要使用手機來存取通信網路30之服務時，各手機要先自動進行網路鎖機制的驗證步驟，以驗證使用者是否為合法使用者。在本發明架構下，此時各手機的處理器就會由該手中的防寫記憶體將解密金鑰讀出，以根據密碼演算法54來將資料記憶體中的密文存取資料解密為明文存取資料，再根據明文存取資料中記錄的網路鎖狀態來驗證使用者是否為合法的使用者。舉例來說，如圖三所示，當

五、發明說明 (16)

手機 32A要進行驗證步驟時，手機 32A的處理器 36就會由資料記憶體 40A、防寫記憶體 50A中分別將密文存取資料 CTA、解密金鑰 DKA讀出，再利用密碼演算法 54，根據解密金鑰 DKA將密文存取資料 CTA解密為一明文存取資料 PTA2。由於密文存取資料 CTA是由服務提供端 49將明文存取資料 PTA以手機 32A之對應加密金鑰 EKA加密而得，而防寫記憶體 50A中的解密金鑰 DKA即對應於加密金鑰 EKA，所以手機 32A由處理器 36解密出來的明文存取資料 PTA2，應該就等於手機 32A原來對應的明文存取資料 PTA。根據處理器 36本身解密出來的明文存取資料 PTA2所記錄的網路狀態，手機 32A就能進行驗證步驟；舉例來說，若明文存取資料 PTA2中記錄手機 32A之網路鎖為啟動，處理器 36就會比對用戶識別卡 45（見圖二）中的用戶識別碼 46是否符合明文存取資料 PTA2中記錄之合法用戶識別碼。若符合，處理器 36就會允許使用者進一步以手機 32A存取通信網路 30的通信服務。不論驗證步驟的結果如何，處理器 36解密而得的明文存取資料 PTA2都只會暫存於處理器 36本身的揮發性記憶區中；等處理器 36完成網路鎖的驗證步驟，也就可將明文存取資料 PTA2釋放，不會暴露於手機 32A的各個非揮發性的記憶體中（像是資料記憶體 40A）。同理，當手機 32B要進行驗證步驟時，手機 32B也會以其防寫記憶體 50B中的專屬解密金鑰 DKB來將資料記憶體 40B中的密文存取資料 CTB解密，以取得對應的明文存取資料 PTB。

本發明以上述的架構來實現網路鎖機制，就可有效保護網路鎖不被破解。如前面所討論過的，在習知技術中，非法使用者可將手機中儲存的網路鎖存取資料（也就是明文的存取資料）以破解存取資料覆蓋，或將其直接竄改，以使習知的手機在進行網路鎖之驗證步驟時，無法得知真正的網路鎖狀態。然而，在本發明中，上述方法都無法破解本發明的網路鎖機制。舉例來說，一意圖破解手機32A網路鎖之非法使用者可將手機32B中的密文存取資料CTB讀出並覆寫至手機32A中，以將手機32A原的密文存取資料CTA用手機32B之密文存取資料CTB代替；但當手機32A要驗證網路鎖而根據解密金鑰DKA將資料記憶體40A中的密文存取資料CTB解密時，由於解密金鑰DKA對應的加密金鑰EKA並非加密密文存取資料CTB的加密金鑰EKB，故處理器36不會解出正確的明文存取資料PTB，其解密出來的明文存取資料PTA2會是沒有意義的，不具有明文存取資料的正確格式（舉例來說，正確明文資料必有一定欄位記錄網路鎖功能是否啟動）。當處理器36發現解密出來的明文存取資料PTA2沒有存取資料的正確格式而是無意義時，就可判斷手機32A之網路鎖已遭破壞。要以手機32B的密文存取資料CTB來破解（代替）手機32A原來的網路鎖，非法使用者必需要將手機32A中的解密金鑰DKA也覆寫為手機32B的解密金鑰DKB，才能讓手機32A以手機32B的解密金鑰DKB將密文存取資料CTB

解密為具有正確格式的明文存取資料；然而，正如前面所強調的，手機32A中的解密金鑰DKA是儲存於防寫記憶體50A中，無法再被覆寫竄改，故非法使用者也無從破解本發明架構下的網路鎖。另外，若非法使用者直接竄改資料記憶體40A中的密文存取資料CTA而意圖破解手機32A的網路鎖，處理器36在驗證步驟中解密出來的明文存取資料PTA2勢必也會變成沒有意義的資料，不具有存取資料的正確格式；此時處理器36也可判斷手機32A的網路鎖遭到破壞。要破解手機32A的網路鎖機制，非法使用者要能將破解的明文存取資料（像是將網路鎖功能記錄為不動之存取資料）以加密金鑰EKA加密為破解的密文存取資料，再覆寫至手機32A中的資料記憶體；但是手機32A的加密金鑰EKA僅保留於通信網路30的網路服務端48，並不會暴露於各手機中，且各手機中的解密金鑰並不等於對應的加密金鑰，故非法使用者將無法得出正確的破解密文存取資料，也就無法破解手機的網路鎖。

當手機32A的處理器36發現解密出來的明文存取資料PTA2沒有正確格式而判斷出網路鎖遭受破壞時，代表密文存取資料CTA已遭不明資料覆寫；此時處理器36可停止手機32A存取通信服務的功能，防止通信網路30的通信秩序及各方的合法權益遭受破壞。另外，在網路鎖受破壞時，處理器32A也可以用人機介面41（於圖二）進一步提示手機32A的使用者需向服務提供端48確認其所應有的權

益；而服務提供端48就可依據手機32A的裝置識別碼IDA於資料庫52中找出手機32A對應的加密金鑰EKA，並依據此機加密金鑰DKA，再以密碼演算法54將明文存取資料PTA加密為密文存取資料CTA，並重新寫入至手機32A中的資料記憶體40A，以恢復手機32A的網路鎖機制。當然，當處理器36發現網路鎖遭到破壞時，也可自動地透過通信網路30向服務提供端48提示其裝置識別碼IDA，並要求服務提供端48透過通信網路將正確的密文存取資料CTA再度傳送至手機32A，由處理器40A自動將其寫入資料記憶體40A中，以恢復手機32A對應的網路鎖機制。由於手機32A僅需密文資料CTA即可恢復網路鎖機制，即使透過無線通信網路傳輸密文存取資料CTA，手機32A加解密金鑰也不會暴露於無線通信網路；此外，即使有非法使用者截獲此密文存取資料CTA，因為各手機對應的解密金鑰皆相異，此密文存取資料CTA也無法用來破解其他手機（像是手機32B）的網路鎖。尤其是當非法使用者以刪除密文存取資料CTA的手段意圖破解手機32A之網路鎖時，手機32A在找不到密文存取資料CTA的情形下，即可向服務提供端48要求再度傳輸密文存取資料CTA，恢復原來的網路鎖機制，保護網路鎖不遭破解。

即使是正常網路鎖內容的改變，以本發明的架構，也可保護網路鎖的安全。舉例來說，若服務提供端48要主動改變手機32A的網路鎖內容（譬如說是將手機32A的

網路鎖由啟動改變為不啟動），網路服務端48可更新明文存取資料PTA，再根據手機32A的加密金鑰EKA將更新後的明文存取資料PTA加密為新的密文存取資料CTA。除了通知手機32A之使用者將手機32A攜至服務提供端48，由服務提供端48（的相關技術人員）將新的密文存取資料CTA寫入至手機32A外，服務提供端48也可透過無線通信網路30將新的密文存取資料CTA傳輸至手機32A，由手機32A的處理器36將其寫入至資料記憶體40A中，代替原來的密文存取資料。這樣一來，不僅能方便手機32A的使用者，由於存取資料在通信網路上傳播時已經加密，也不...擔心密文存取資料的暴露危害各手機的網路鎖安全。另外，在各手機的明文存取資料中，除了記錄對應手機的網路鎖狀態外，還能另外再於明文存取資料後，除了記錄該手機含了該手機的裝置識別碼，使加密後的密文存取資料中，除了記錄該手機含了該手機的裝置識別碼。當該手機進行認證步驟明文存取資料的裝置識別碼及該手機真正的依據明文存取資料是否正確格式來判斷網路鎖是否遭破壞，也可比對解密出來的裝置識別碼，判斷網路鎖機制是否遭到破壞。

總結來說，在習知技術中，由於網路鎖存取資料是以明文方式記錄於各手機中，易遭非法使用者以覆寫、直接竄改等方式加以破解，影響網路通信秩序及各方的

合法權益。相較之下，本發明是對通信網路中的各手機分配一組獨一無二的加解密金鑰，網路服務端保留各手機對應的加密金鑰，以將各手機對應網路鎖之明文存取資料加密為對應的密文存取資料。而各手機僅保留密文存取資料，並以防寫、唯讀的方式記錄有對應的解密金鑰。當一手機要進行網路鎖之認證步驟時，係以該手機之解密金鑰將該密文存取資料解密為明文存取資料，再依據明文存取資料實現網路鎖機制。由於各手機的加解密金鑰不相同，即使非法使用者以其他手機的密文存取資料覆寫一手機的密文存取資料，該手機都會發現網路鎖遭破壞而阻止對通信服務的非法存取，進而達到保護網路鎖機制的目的，維護通信網路的通信秩序及各方的合法權益。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明專利之涵蓋範圍。

## 圖式之簡單說明

圖一為一習知通信網路中各手機及服務提供端相關配置的示意圖。

圖二為本發明通信網路中各手機及服務提供端相關配置的示意圖。

圖三為本發明網路鎖機制實施情形之示意圖。

## 圖式之符號說明

| | | | |
|---|---|---|---|
| 10、30 | 通信網路 | | |
| 12-13、32A-32B | 手機 | | |
| 14、34 | 收發模組 | 16、36 | 處理器 |
| 18A、38A | 麥克風 | 18B、38B | 揚聲器 |
| 20、40A-40B | 資料記憶體 | | |
| 21、41 | 人機介面 | 22 | 存取資料 |
| 23、IDA-IDB | 裝置識別碼 | | |
| 24、45 | 用戶識別卡 | 26、46 | 用戶識別碼 |
| 28、48 | 服務提供端 | 29、49 | 基地台 |
| 50A-50B | 防寫記憶體 | 52 | 資料庫 |
| 54 | 密碼演算法 | EKA-EKB | 加密金鑰 |
| DKA-DKB | 解密金鑰 | PTA-PTB | 明文存取資料 |
| CTA-CTB | 密文存取資料 | | |

六、申請專利範圍

1. 一種使用於一通信網路的方法，用來識別該通信網路中一通信裝置是否可存取該通信網路的通信服務，其中該通信裝置包含有：

一資料記憶體，用來記錄一密文存取資料；以及

一防寫記憶體，用來以非揮發性的方式記錄一解密金鑰；

其中該防寫記憶體中記錄的資料不能被覆寫，使得即使該資料記憶體中記錄的資料被改變，該防寫記憶體中記錄之解密金鑰也不會被改變；

而該方法包含有：

進行一驗證步驟，以讀取該防寫記憶體中之解密金鑰及讀取該資料記憶體中之密文存取資料；

再根據該解密金鑰，以一預設之密碼演算法將該密文存取資料解密為一明文存取資料，並根據該明文存取資料，判斷該通訊裝置是否可存取該通訊網路之通信服務。

2. 如申請專利範圍第 1項之方法，其中該密碼演算法為一非對稱(asymmetric)之加解密演算法。

如申請專利範圍第 1項之方法，其中該資料記憶體為一非揮發性的記憶體。

4. 如申請專利範圍第 1項之方法，其另包含有：

根據一加密金鑰，將一對應該通信裝置的存取資料以該密碼演算法加密為該密文存取資料；其中該加密金鑰係對應於該解密金鑰，使得一明文在根據該加密金鑰以該密碼演算法加密為一密文後可根據該解密金鑰解密為原來之明文；以及

將該密文存取資料記錄至該資料記憶體。

5. 如申請專利範圍第4項之方法，其另包含有：

在根據該加密金鑰加密出該密文存取資料前，根據該密碼演算法產生出該加密金鑰及該對應之解密金鑰。

6. 如申請專利範圍第4項之方法，其中該通信網路中另包含有一服務提供端，用來對該通信裝置提供通信服務；該服務提供端設有一資料庫，用來記錄該加密金鑰及對應該通信裝置的存取資料。

7. 如申請專利範圍第6項之方法，其中當根據該加密金鑰加密出該密文存取資料時，係於該服務提供端根據該資料庫中記錄之加密金鑰將對應該通信裝置的存取資料加密為該密文存取資料。

8. 如申請專利範圍第7項之方法，其中當要將該密文存取資料記錄至該資料記憶體時，係將該密文存取資料由該服務提供端透過該通信網路傳輸至該通信裝置，再以

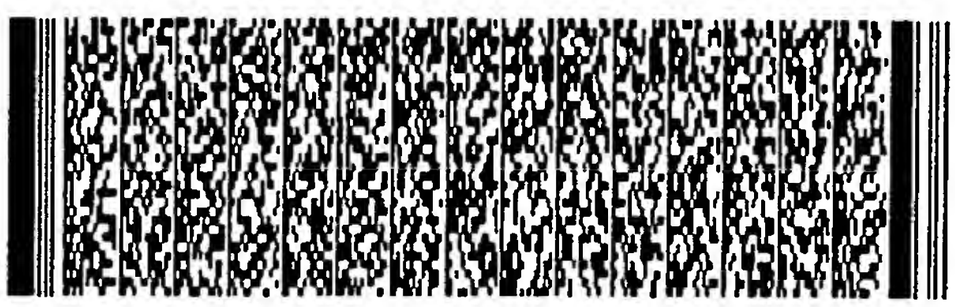
該通信裝置將該密文存取資料記錄至該資料記憶體。

9. 如申請專利範圍第4項之方法，其中該加密金鑰與該解密金鑰相異。

10. 如申請專利範圍第1項之方法，其中當根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該明文存取資料是否符合一預設存取資料來判斷；若該明文存取資料符合該預設存取資料，則判斷該通信裝置可存取該通信網路之通信服務；若否，則判斷該通信裝置不可存取該通信網路之通信服務，而該通信裝置會停止存取該通信網路。

11. 如申請專利範圍第1項之方法，其中該通信裝置中另包含有一用戶識別卡，用來記錄一用戶識別碼；而該明文存取資料中記錄有一預設識別碼；其中當根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該用戶識別碼是否符合該預設識別碼來判斷；若兩者符合，則判斷該通信裝置可存取該通信網路之通信服務；若否，則判斷該通信裝置不可存取該通信網路之通信服務，而該通信裝置會停止存取該通信網路。

12. 如申請專利範圍第1項之方法，其中該通信裝置為一手機，而該通信網路為一無線通信網路。



六、申請專利範圍

13. 一種用於一通信網路中的通信裝置，用來存取取該通信網路的通信服務；該通信裝置包含有：

一資料記憶體，用來以非揮發性的方式記錄一密文存取資料；

一防寫記憶體，用來以非揮發性的方式記錄一解密金鑰；

其中該防寫記憶體中記錄的資料不能被覆寫，使得即使該資料記憶體中記錄的資料被改變，該防寫記憶體中記錄之解密金鑰也不會被改變；

一處理器，用來控制該通信裝置的運作；

其中當該通信裝置要存取該通信網路之通信服務前，該處理器會進行一驗證步驟，以讀取該防寫記憶體中之解密金鑰及讀取該資料記憶體中之加密存取資料；再根據該解密金鑰，以一預設之密碼演算法將該密文存取資料解密為一明文存取資料，並根據該明文存取資料，判斷該通訊裝置是否可存取該通訊網路之通信服務。

14. 如申請專利範圍第 13項之通信裝置，其中該密碼演算法為一非對稱（asymmetric)之加解密演算法。

15. 如申請專利範圍第 13項之通信裝置，其中該資料記憶體為一非揮發性的記憶體。

六、申請專利範圍

16. 如申請專利範圍第13項之通信裝置，其中該通信網路中另包含有一服務提供端，用來對該通信裝置提供通信服務；該服務提供端設有一資料庫，用來記錄一加密金鑰及對應該通信裝置的存取資料；而該通信裝置中的密文存取資料係根據該加密金鑰，將對應該通信裝置的存取資料以該密碼演算法加密而得；其中該加密金鑰係對應於該解密金鑰，使得一明文在根據該加密金鑰以該密碼演算法加密為一密文後可根據該解密金鑰解密為原來之明文。

17. 如申請專利範圍第16項之通信裝置，其中該加密金鑰及該對應之解密金鑰係根據該密碼演算法所計算出來的。

18. 如申請專利範圍第16項之通信裝置，其中將該密文存取資料係由該服務提供端透過該通信網路傳輸至該通信裝置，再由該處理器將該密文存取資料記錄至該資料記憶體。

19. 如申請專利範圍第13項之通信裝置，其中當該處理""根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該明文存取資料是否符合一預設存取資料來判斷；若該明文存取資料符合該預設存取資料，則該處理器會判斷該通信裝置可存取該通信

網路之通信服務。

20. 如申請專利範圍第13項之通信裝置，其中該通信裝置中另包含有一用戶識別卡，用來記錄一用戶識別碼；而該明文存取資料中記錄有一預設識別碼；其中當該處理器根據該明文存取資料判斷該通信裝置是否可存取該通信網路之通信服務時，係根據該用戶識別碼是否符合該預設識別碼來判斷；若兩者符合，則判斷該通信裝置可存取該通信網路之通信服務；若否，則判斷該通信裝置不可存取該通信網路之通信服務，而該通信裝置會停止存取該通信網路。

21. 如申請專利範圍第13項之通信裝置，其係為一手機，而該通信網路為一無線通信網路。

22. 一種使用於一通信網路的方法，其中該通信網路包含有：

複數個通信裝置，每一通信裝置包含有一防寫記憶體及一資料記憶體；

而該方法係用來驗證各通信裝置是否可存取該通信網路之通信服務；該方法包含有：

根據一密碼演算法，提供複數個相異的加密金鑰及複數個解密金鑰，其中各加密金鑰對應於一解密金鑰；

使得一明文在根據一加密金鑰以該密碼演算法加密

為一密文後可根據該加密金鑰對應之解密金鑰解密為原來之明文；

使不同的通信裝置對應於不同的加密金鑰；

將每一通信裝置對應的一筆存取資料根據該通信裝置對應之加密金鑰以該密碼演算法加密為一密文存取資料；

將對應每一通信裝置加密金鑰之解密金鑰記錄於該通信裝置中的防寫記憶體，以使該解密金鑰不會被覆寫；

將每一通信裝置的密文存取資料記錄於該通信裝置的資料記憶體；以及

當要驗證一通信裝置是否可存取該通信網路之通信服務時，根據該通信裝置防寫記憶體中之解密金鑰以該密碼演算法將該通信裝置資料記憶體中之密文存取資料解密，並根據解密後之密文存取資料來判斷該通信裝置是否可存取該通信網路之通信服務。

23. 如申請專利範圍第22項之方法，其中不同之加密金鑰對應之解密金鑰也互不相同。

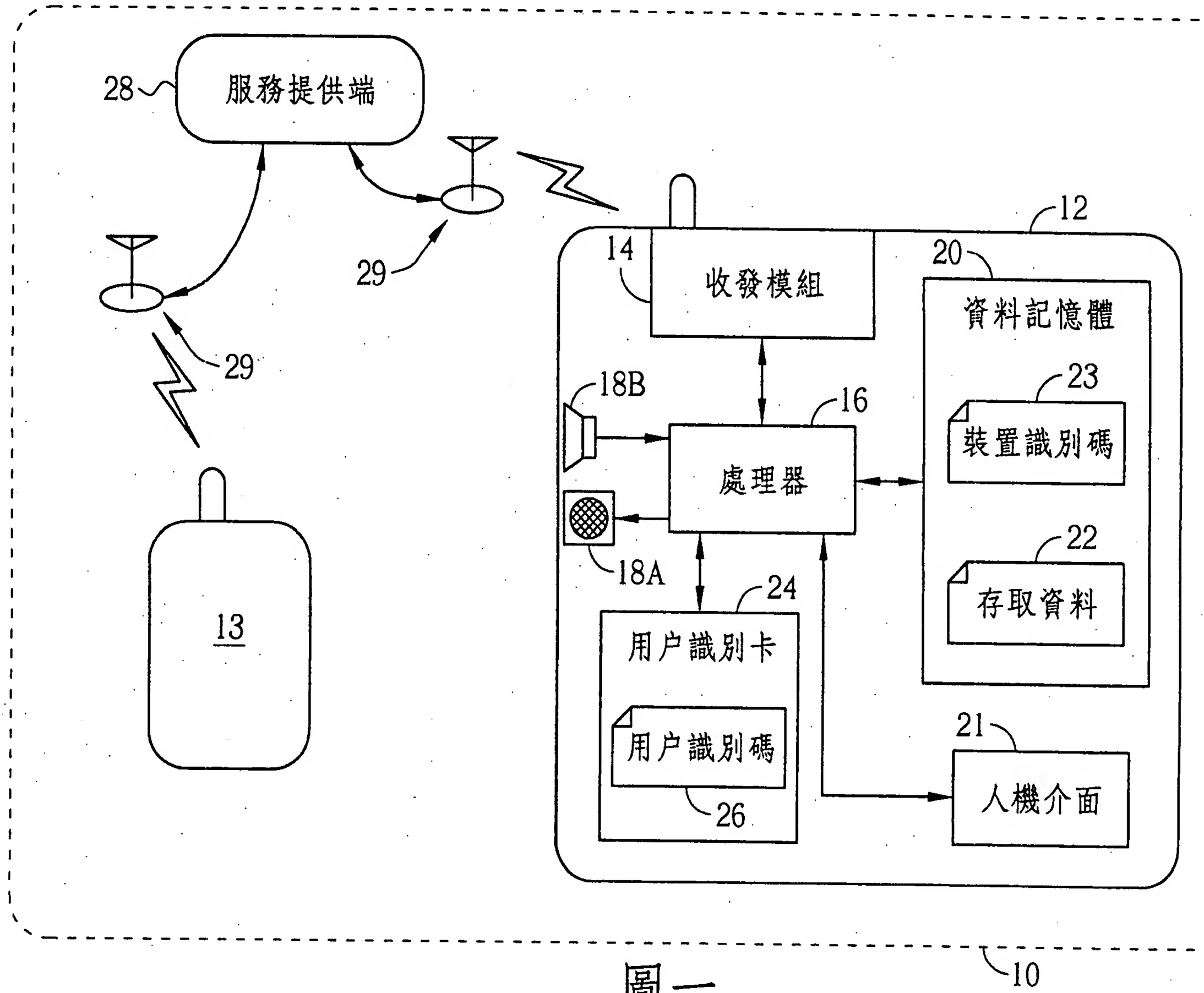
24. 如申請專利範圍第22項之方法，其中該密碼演算法係一非對稱之加解密演算法，使一加密金鑰與對應之解密金鑰不相等；而當一明文根據該加密金鑰以該密碼演算法加密為一密文後，該密文無法根據該加密金鑰以該

密碼演算法解密為原來之明文。

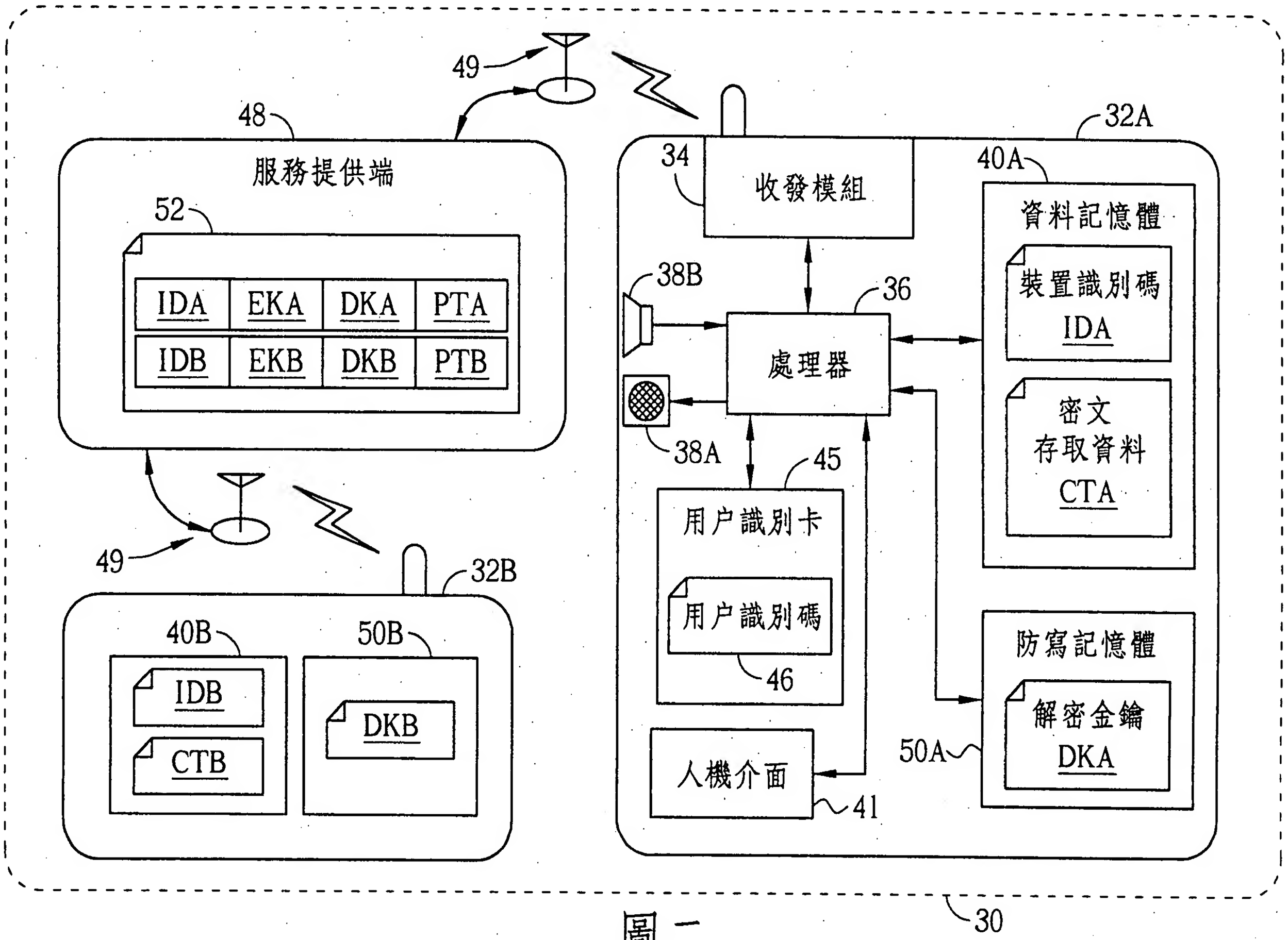
25. 如申請專利範圍第22項之方法，其中該通信網路另包含有一服務提供端，用來在各通信裝置間傳輸訊號以提供通信服務；該服務提供端設有一資料庫，而該方法另包含有：

將各通信裝置對應之加密金鑰記錄於該資料庫中。

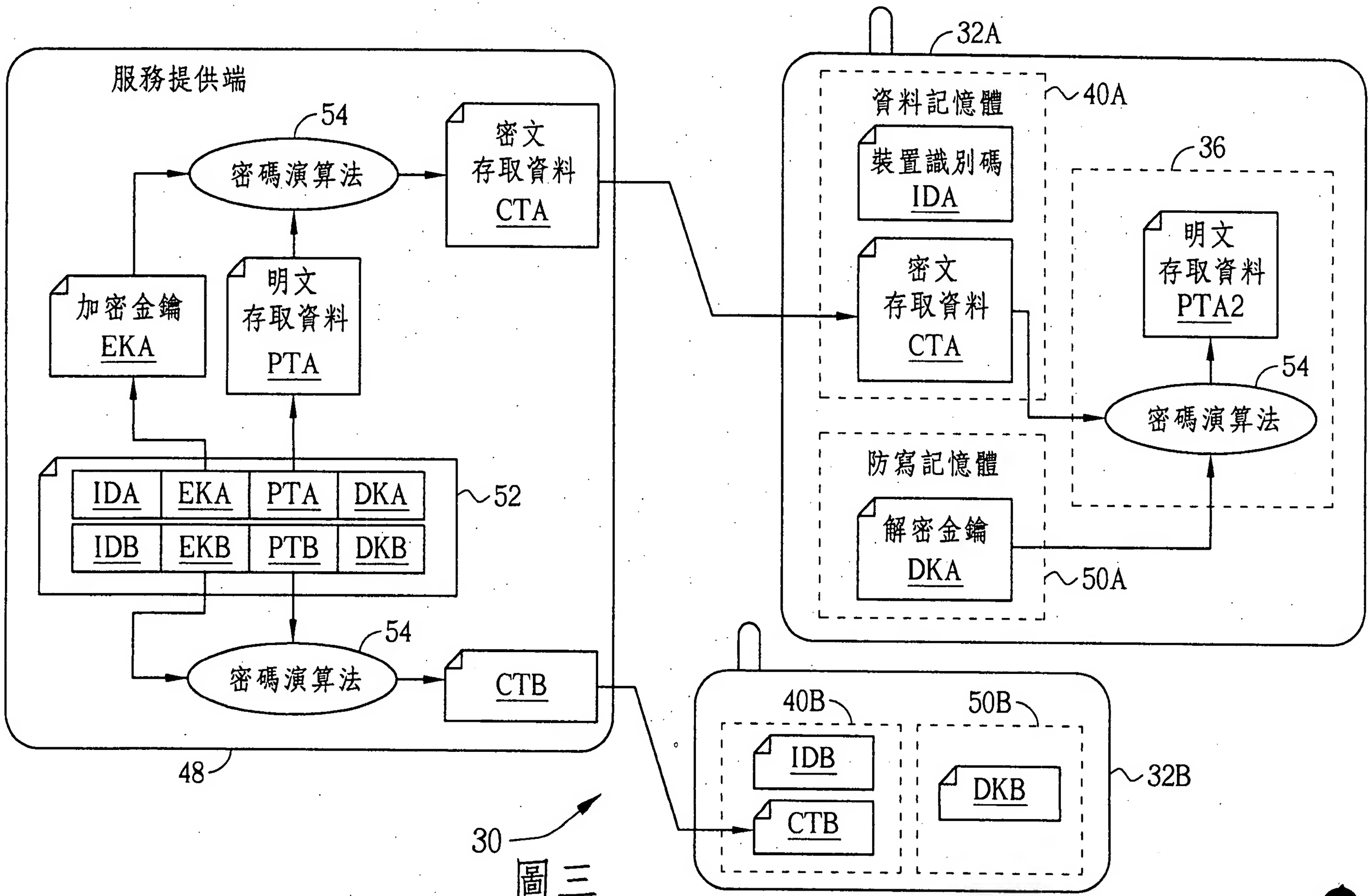
26. 如申請專利範圍第22項之方法，其中該等通信裝置為手機，而該通信網路為一無線通信網路。


28
服務提供端
29
29
13
12
14
收發模組
20
資料記憶體
23
裝置識別碼
18B
16
處理器
22
存取資料
18A
24
用户識別卡
用户識別碼
26
21
人機介面
10

圖一


49
48
服務提供端
52
IDA
EKA
DKA
PTA
IDB
EKB
DKB
PTB
49
32B
40B
50B
IDB
CTB
DKB
32A
34
收發模組
40A
資料記憶體
裝置識別碼
IDA
密文
存取資料
CTA
38B
36
處理器
38A
45
用户識別卡
用户識別碼
46
防寫記憶體
解密金鑰
DKA
50A
人機介面
41
30

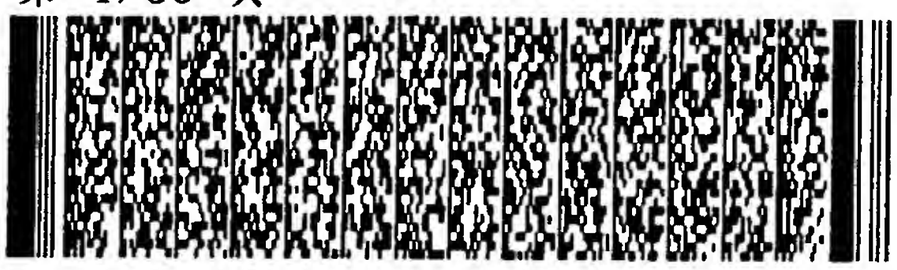
圖二


服務提供端
54
密碼演算法
密文
存取資料
CTA
加密金鑰
EKA
明文
存取資料
PTA
IDA
EKA
PTA
DKA
IDB
EKB
PTB
DKB
52
54
密碼演算法
CTB
48
30
32A
資料記憶體
40A
裝置識別碼
IDA
密文
存取資料
CTA
36
明文
存取資料
PTA2
54
密碼演算法
防寫記憶體
解密金鑰
DKA
50A
40B
50B
IDB
CTB
DKB
32B

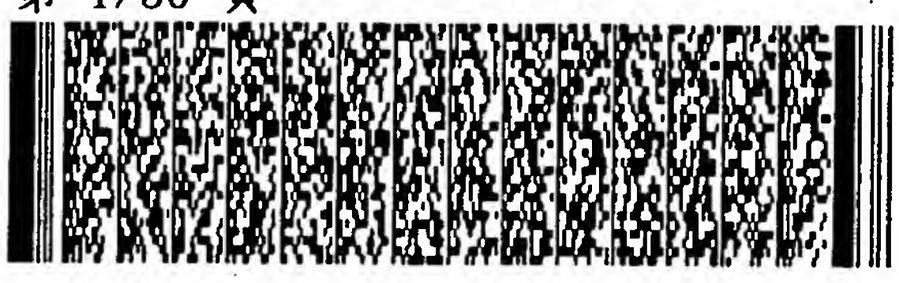
圖三

申請案件名稱:以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置

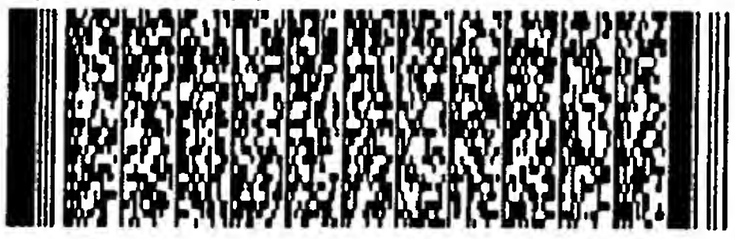
第 1/36 頁



第 1/36 頁

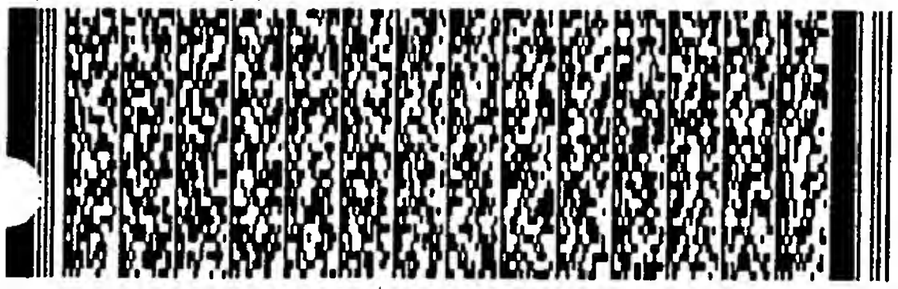


第 2/36 頁

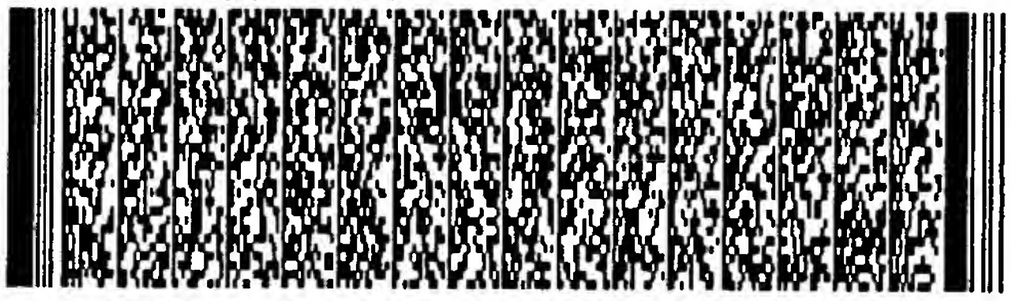


第 3/36 頁

第 3/36 頁



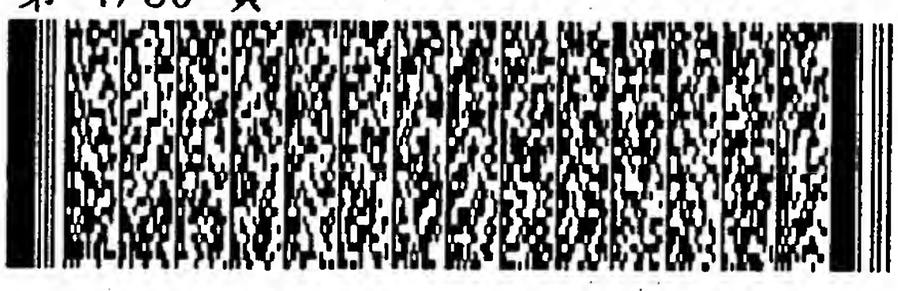
第 4/36 頁



第 5/36 頁

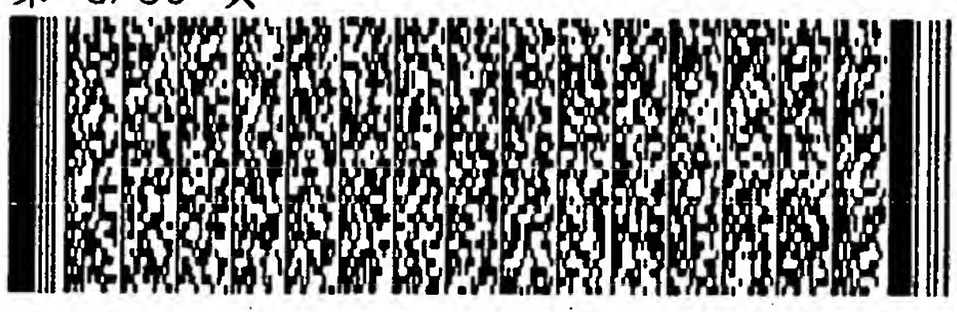
第 6/36 頁

第 7/36 頁

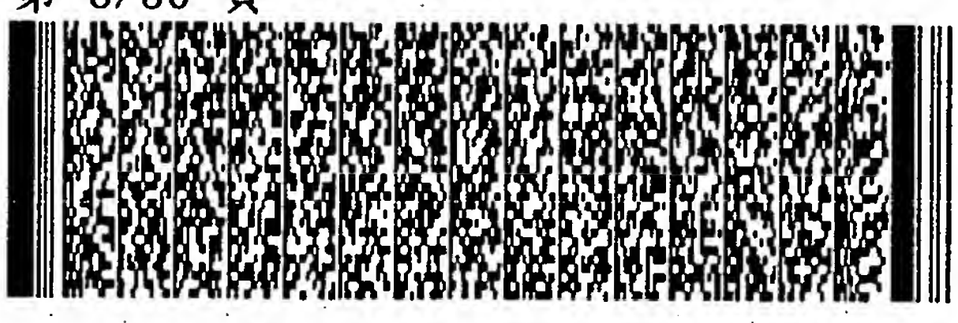


第 7/36 頁

第 8/36 頁



第 8/36 頁



第 9/36 頁

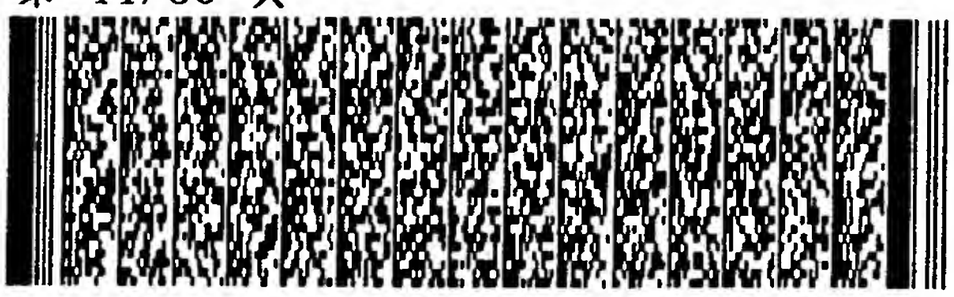
第 9/36 頁

第 10/36 頁

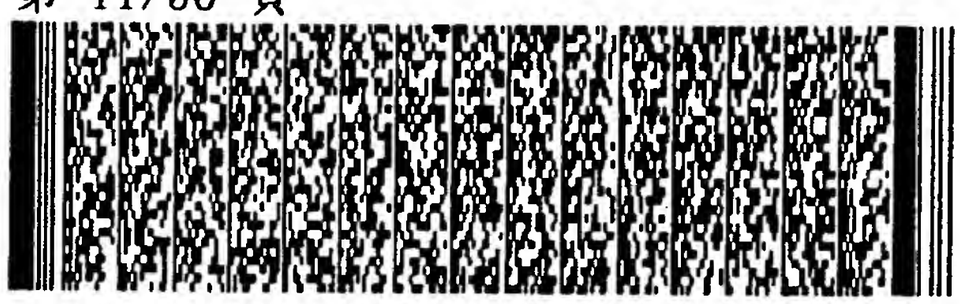
第 10/36 頁

申請案件名稱:以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置

第 11/36 頁

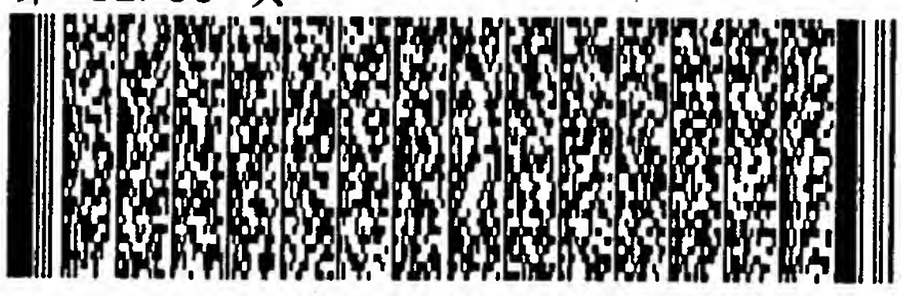


第 11/36 頁

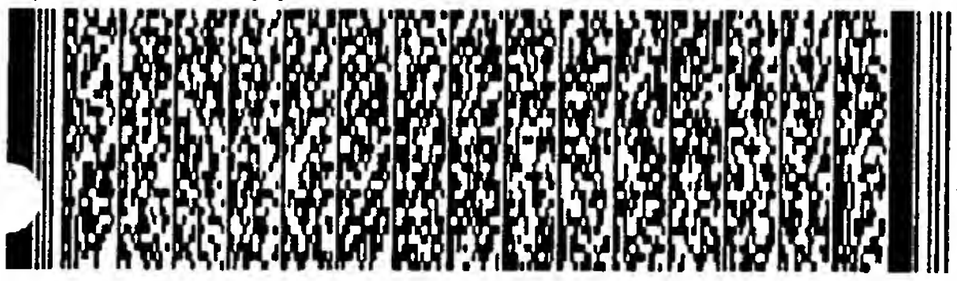


第 12/36 頁

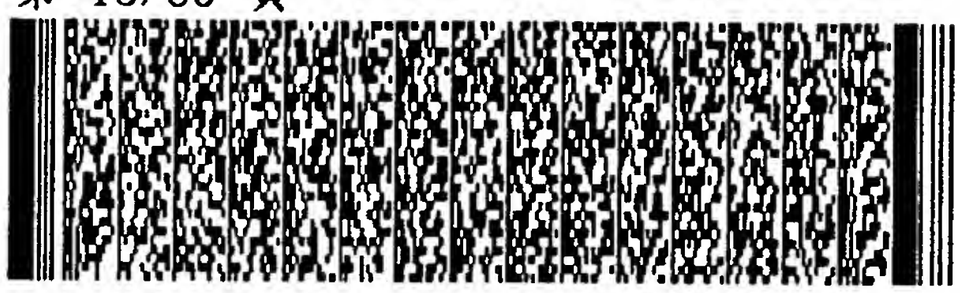
第 12/36 頁



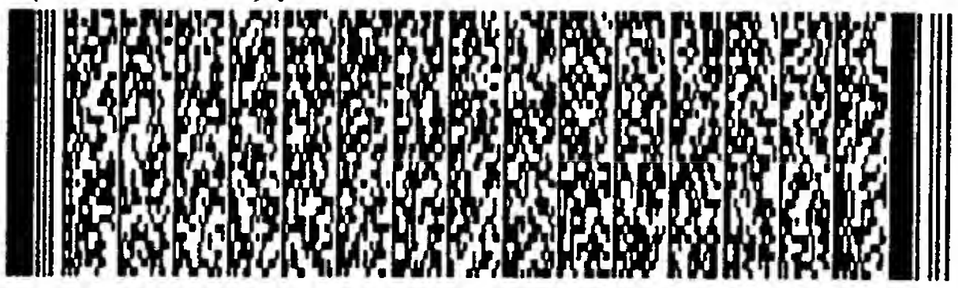
第 13/36 頁



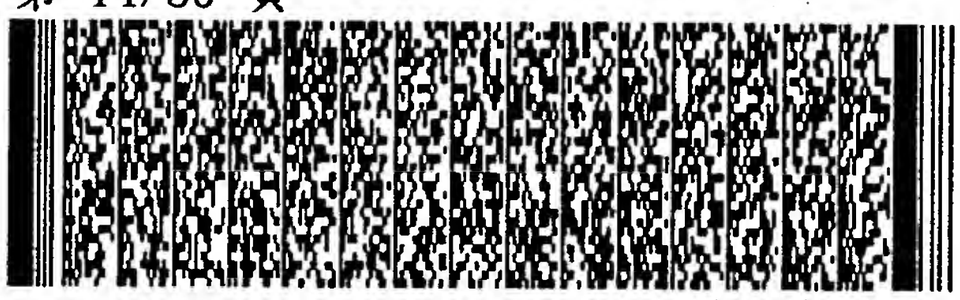
第 13/36 頁



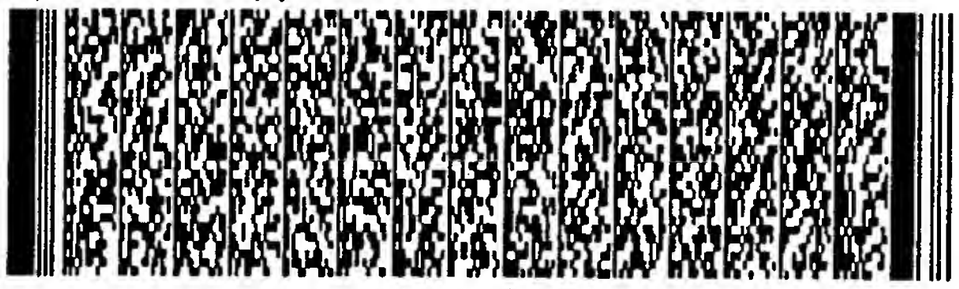
第 14/36 頁



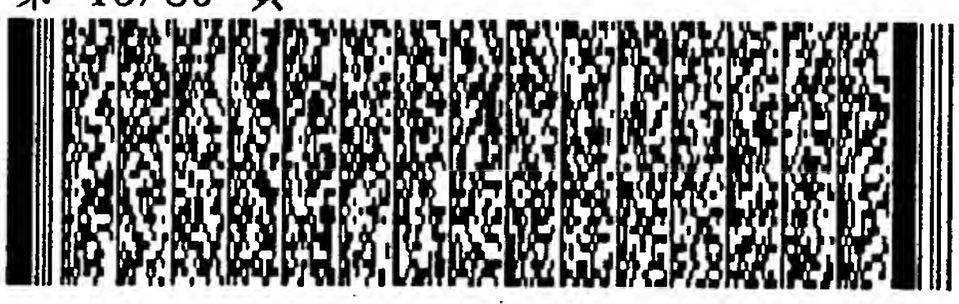
第 14/36 頁



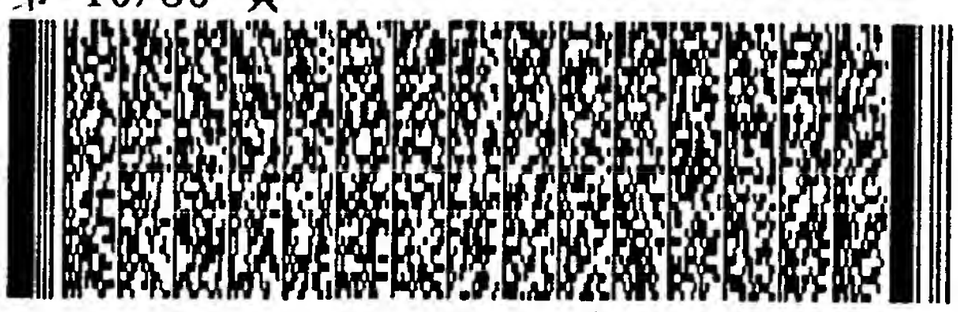
第 15/36 頁



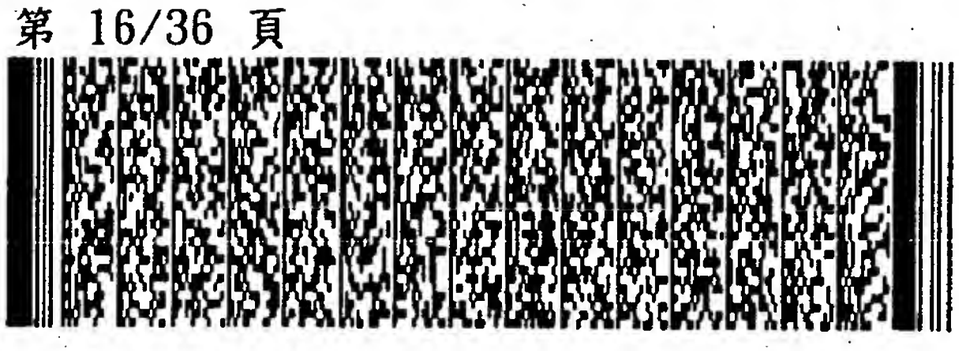
第 15/36 頁



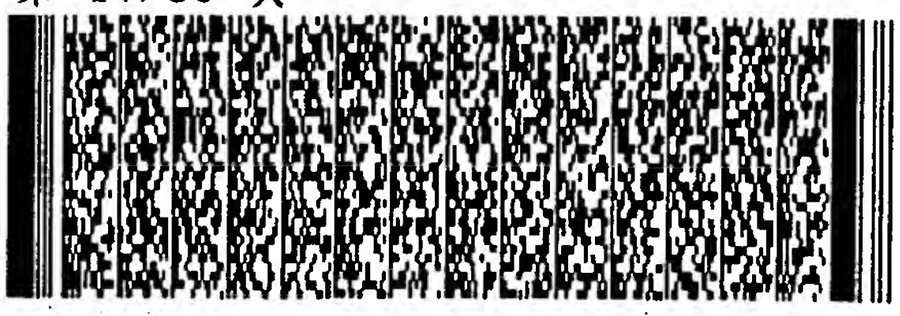
第 16/36 頁



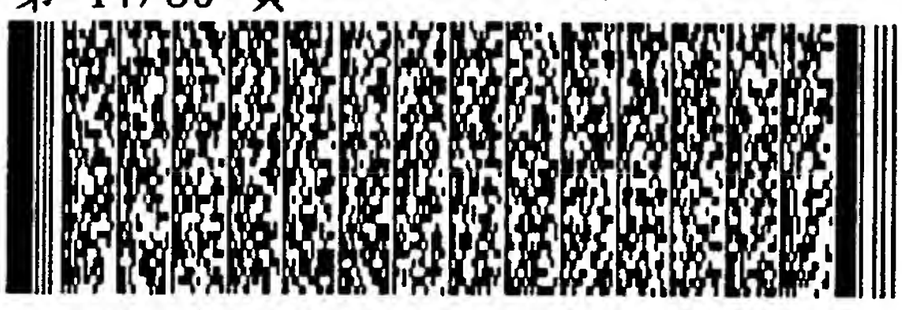
第 16/36 頁



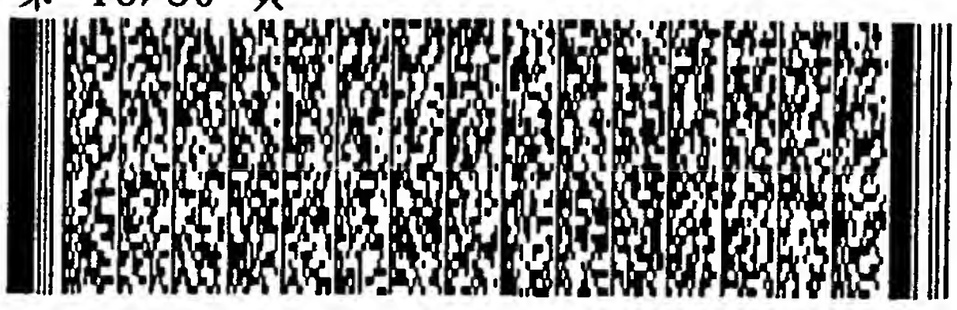
第 17/36 頁



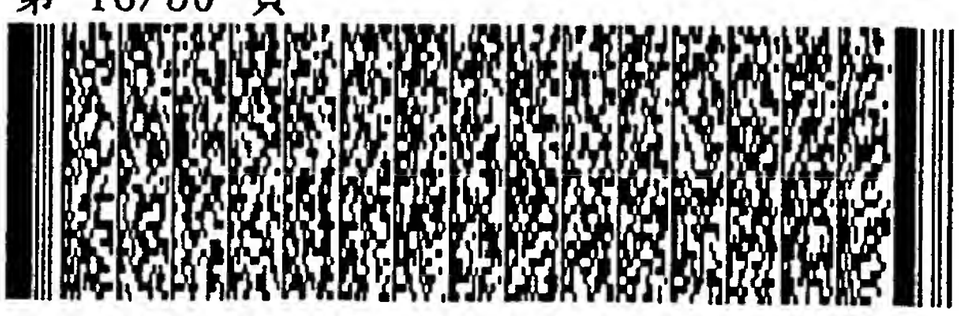
第 17/36 頁



第 18/36 頁

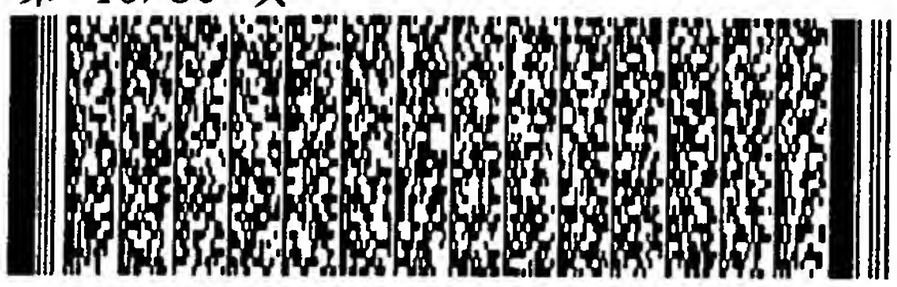


第 18/36 頁

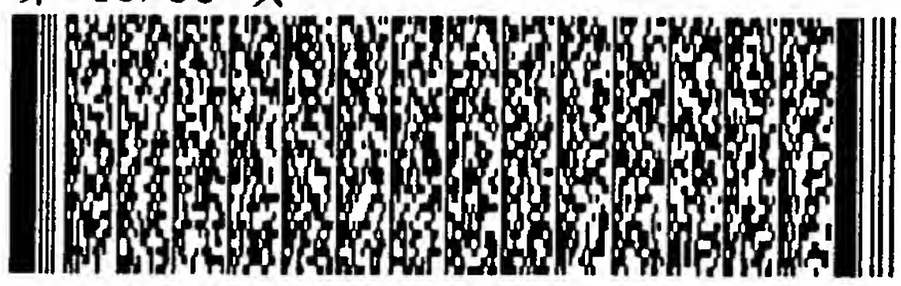


申請案件名稱:以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置

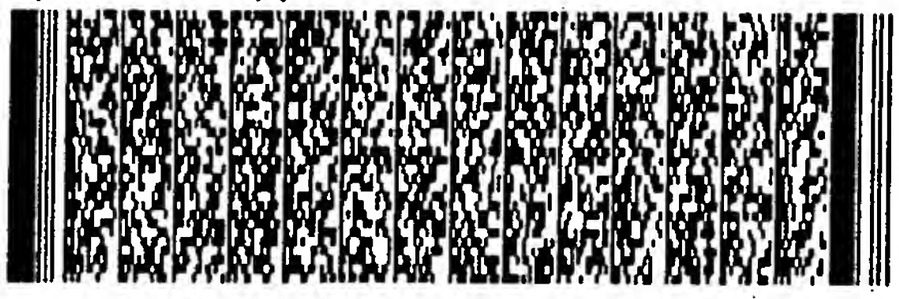
第 19/36 頁



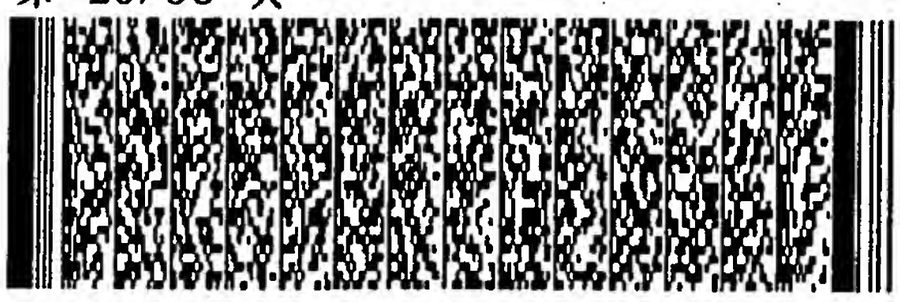
第 19/36 頁



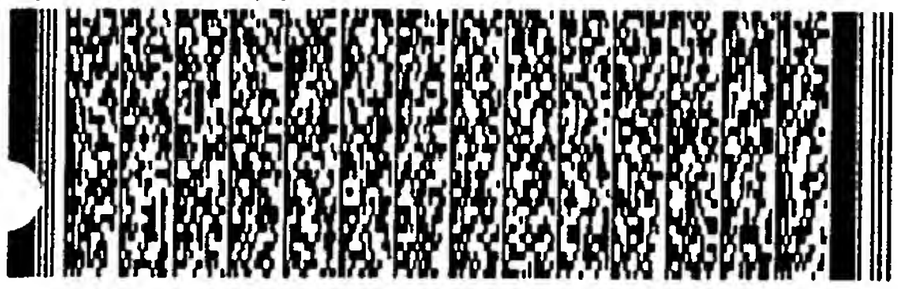
第 20/36 頁



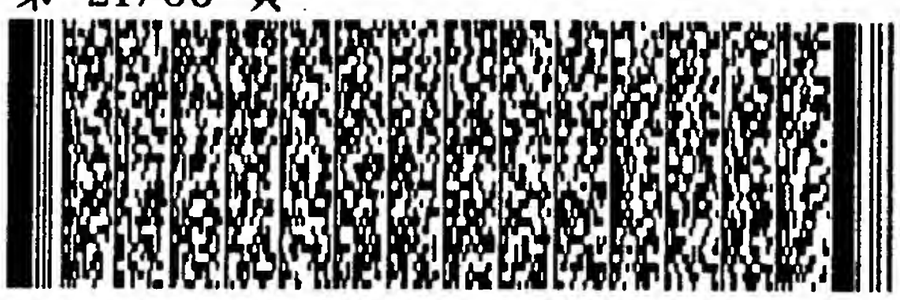
第 20/36 頁



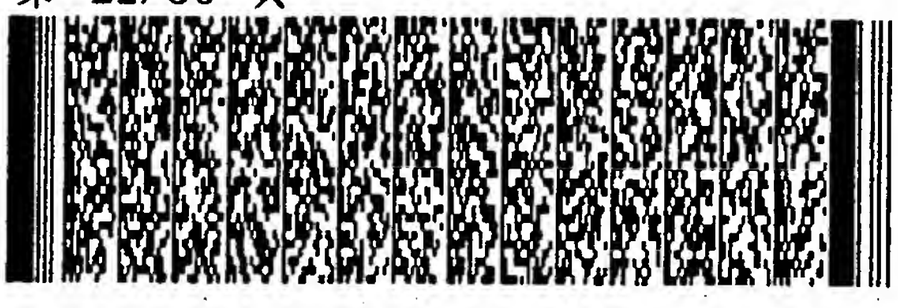
第 21/36 頁



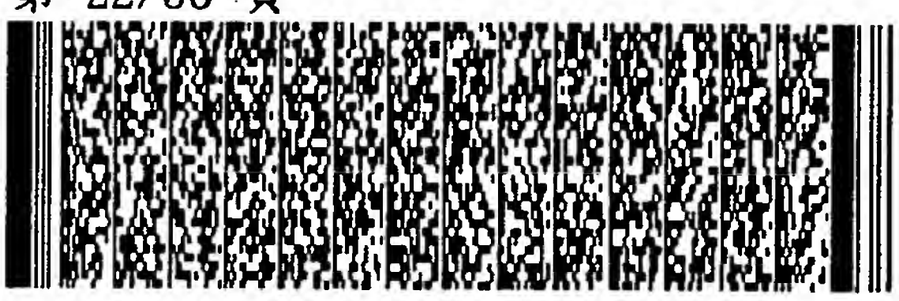
第 21/36 頁



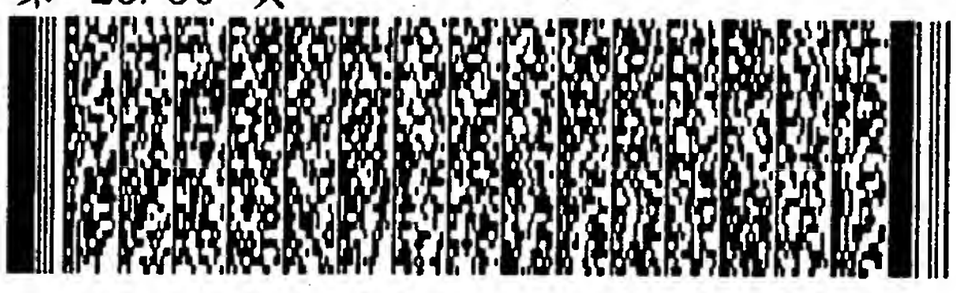
第 22/36 頁



第 22/36 頁

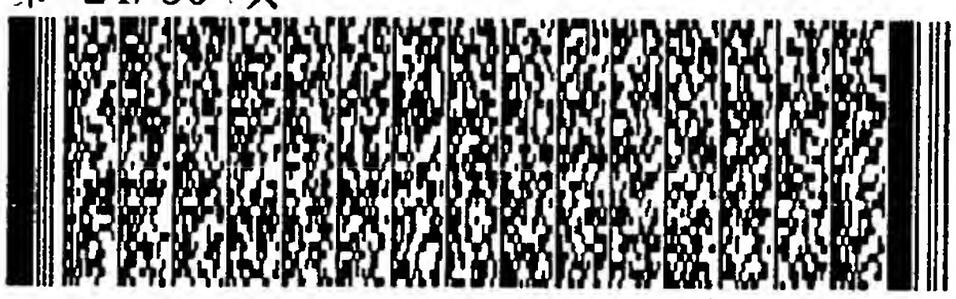


第 23/36 頁



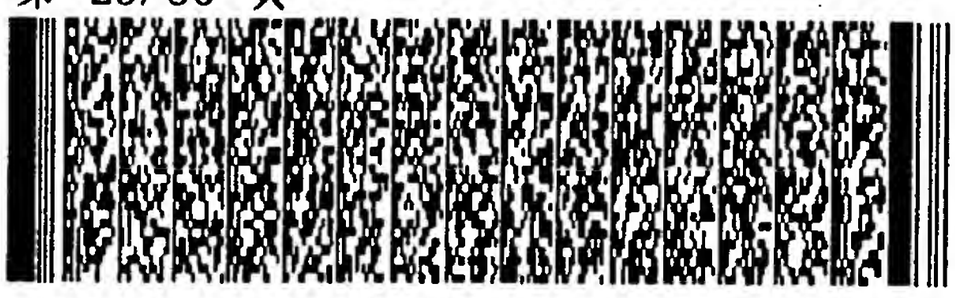
第 23/36 頁

第 24/36 頁

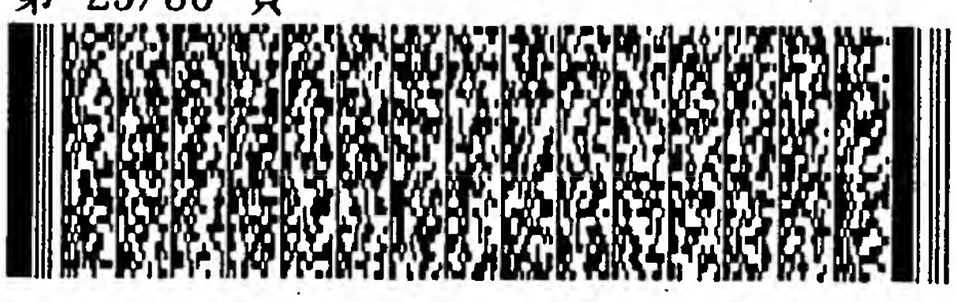


第 24/36 頁

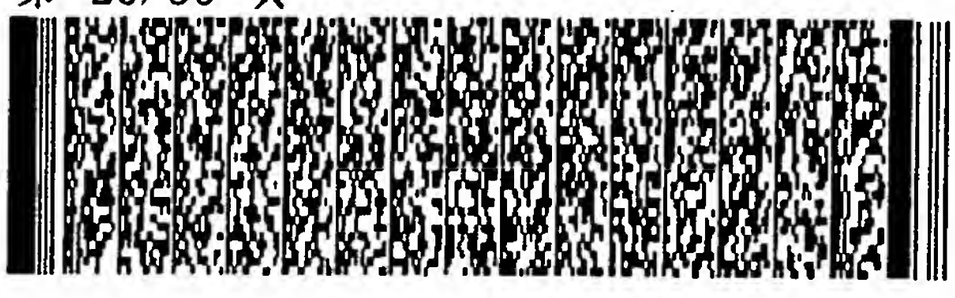
第 25/36 頁



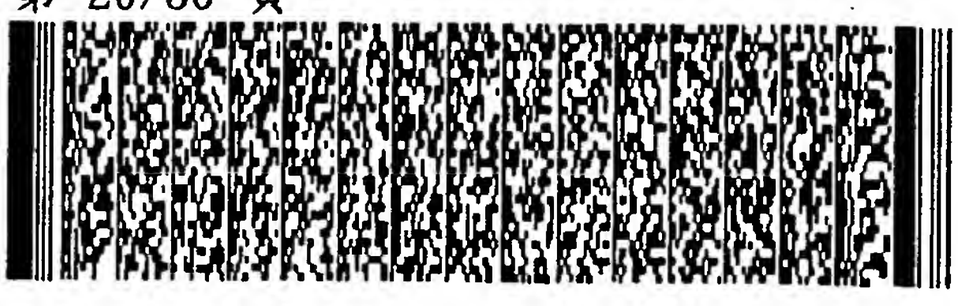
第 25/36 頁



第 26/36 頁

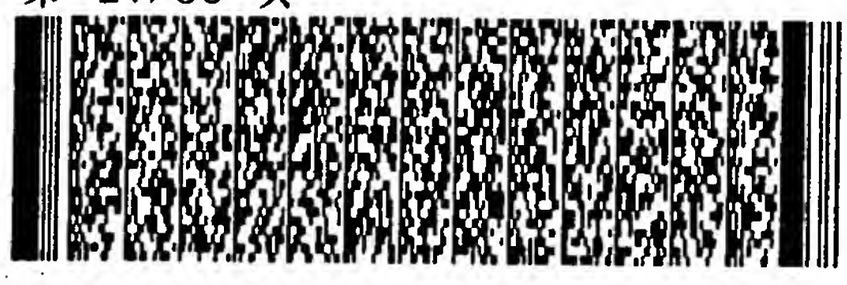


第 26/36 頁

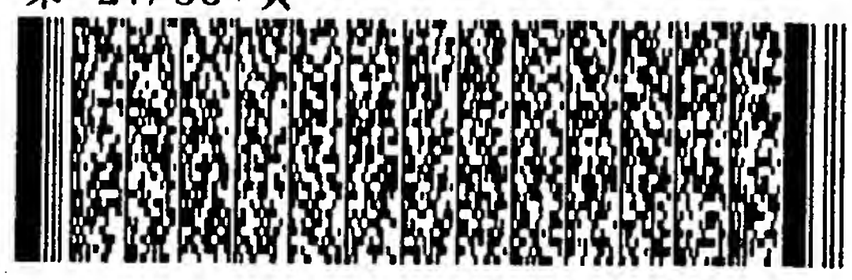


申請案件名稱:以防寫解密金鑰防止手機加密網路鎖被破解之保護方法及相關裝置

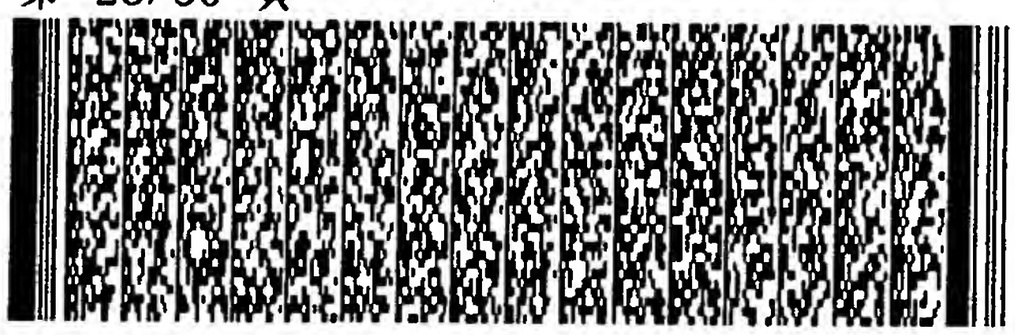
第 27/36 頁



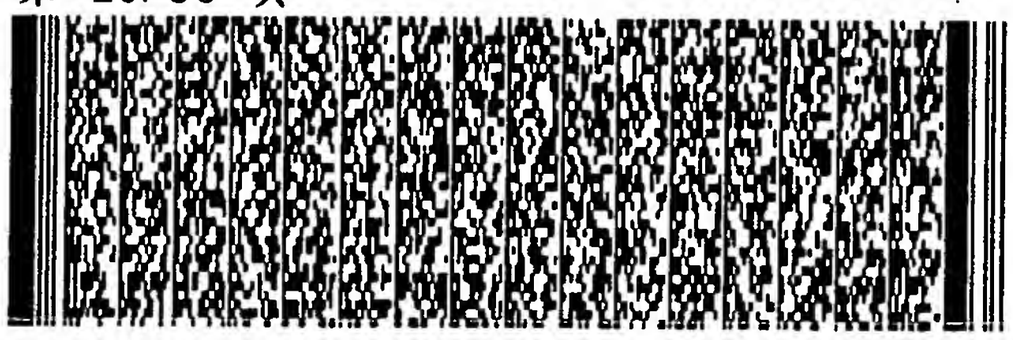
第 27/36 頁



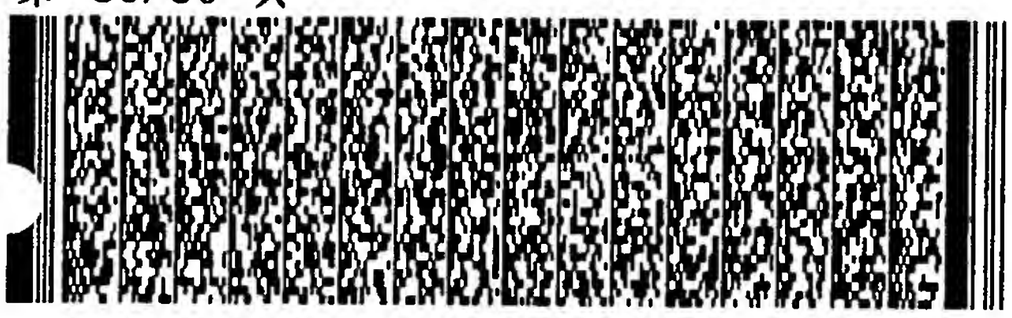
第 28/36 頁



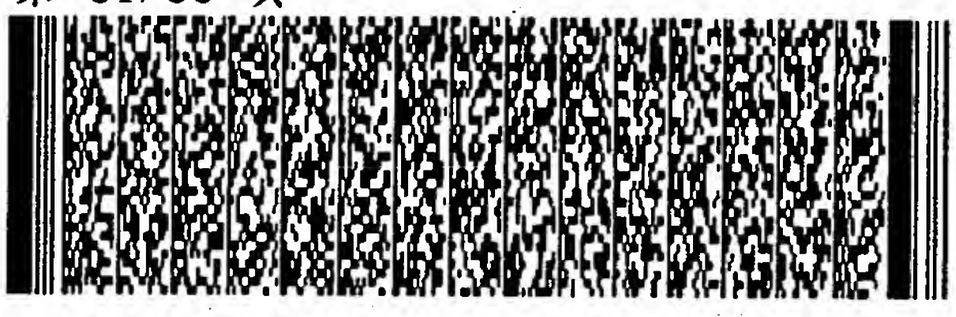
第 29/36 頁



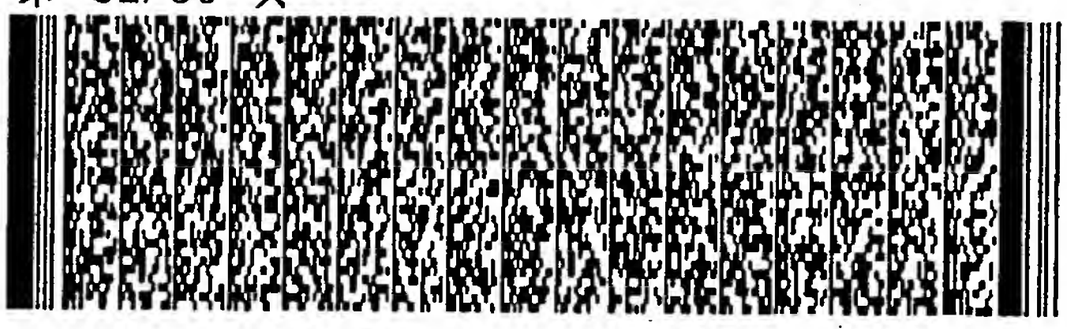
第 30/36 頁



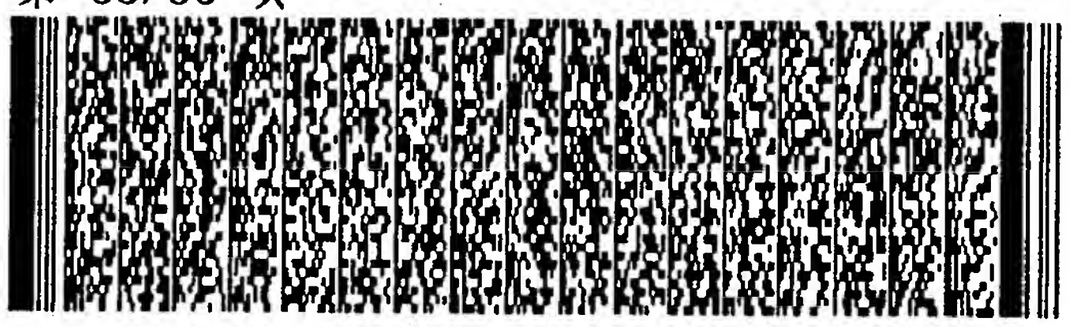
第 31/36 頁



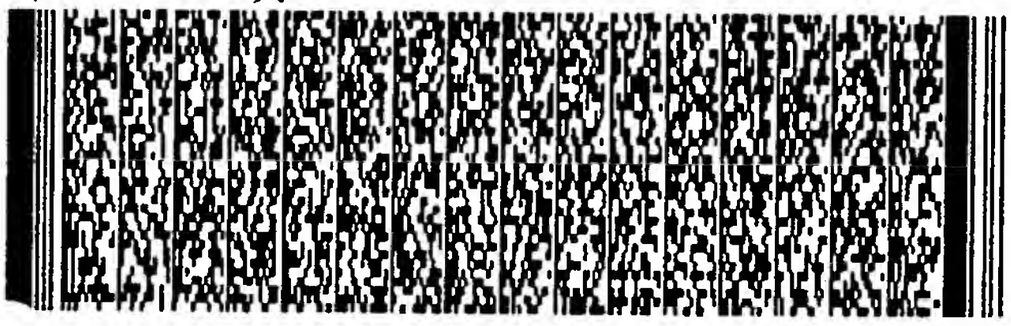
第 32/36 頁



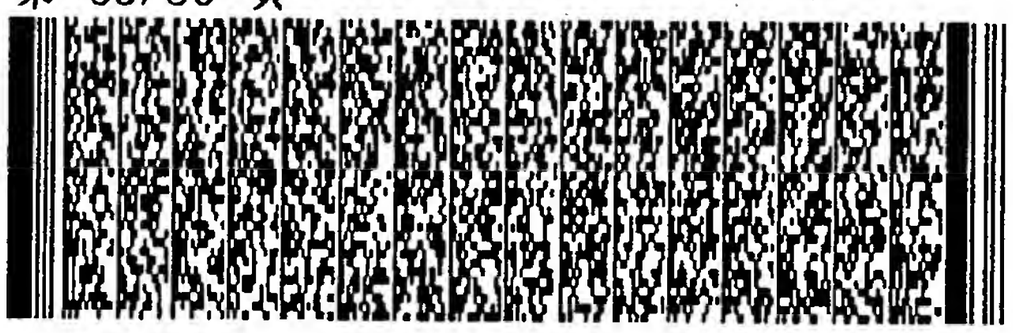
第 33/36 頁



第 34/36 頁



第 35/36 頁



第 36/36 頁